Financial Crime Tradecraft: A Critical Study of the Mechanics of Financial Crime

Douglas M. C. Allan

A thesis submitted for the degree of

Doctor of Philosophy in the

School of Regulation, Justice and Diplomacy

The Australian National University

December 2021

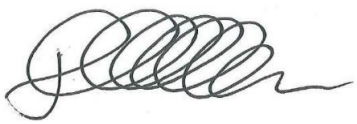
Copyright by [Douglas M C Allan] [2021]

All Rights Reserved

Candidate Declaration

This thesis is a record of research undertaken between February 2013 and December 2021 at the Regulatory Institutions Network, the School of Regulation, Justice and Diplomacy, the Australian National University, Canberra, Australia.

I certify that this thesis is an original work that does not contain, without appropriate acknowledgement, any material previously submitted in whole or part for any degree at any University. Furthermore, to the best of my knowledge and belief, it does not contain any material previously published or written by any other person except where due reference is made in the text.



……

Douglas M C Allan

December 2021

Mo toku whanau

Acknowledgements

That I am fortunate enough to write this acknowledgement is a testament to the energy of those who supported me on this journey.

It is with genuine candour that I acknowledge the expertise, support and patience of Emeritus Professor Roderic Broadhurst who pushed me to continually hone my thinking along this journey. Your forthright and honest approach was instrumental in me achieving this outcome.

I would like to thank Emeritus Professor Peter Grabosky, Dr Emmeline Taylor and Dr Christopher Devery, who at different times have provided critical, yet helpful feedback. From the initial proposal to the completed thesis, the support of this supervisory panel led by Professor Broadhurst has in equal measure challenged and supported my research.

This thesis would not have been possible without the support of the Australian Federal Police and the New South Wales Police Force. From the Detective Constable to the Commander, the professionalism and expertise of these highly knowledgeable individuals are testaments to their organisations and the broader Australian community they serve. The commitment and pride they have in their work make these law enforcement officers some of the finest in the world. I would also like to thank the staff at the New South Wales Police Force Academy for their support in transcribing seemingly endless hours of interviews. This thesis was edited by Elite Editing, and editorial intervention was restricted to Standards D and E of the Australian Standards for Editing Practice. The editor's current or former area of academic specialisation is not similar to this thesis nor that of the researcher.

Finally, I would like to thank my family. To Rachel and Indira, thank you for your patience and for allowing me space. To my mother, sister, brother and uncle, thank you. To my late father, I miss you.

Abstract

This thesis contributes to understanding of the tradecraft of fraudsters who commit complex financial crimes. It takes up the challenge laid down by Levi (1984) and Braithwaite (1985) to give greater attention to how fraudsters commit their crimes. It provides insight into the diversity of tradecraft regularly applied by fraudsters in pursuit of their objectives. The underlying hypothesis of this thesis is that a fraudster's status as either an insider or an outsider of a target financial system influences how they deploy their tradecraft.

This thesis proposes the presence of three interlinked activity domains common to all complex financial crimes. It found the access, learning and planning domains, when combined, produce a process model that enables the testing of the hypothesis driving this research. The data—primarily transcripts of interviews with detectives and criminal case management files—are divided into insider and outsider cases. These cases are thematically analysed to identify key similarities and differences in the methods, resources and tradecraft used by fraudsters. This process identifies key stages in the commission of financial crime including accessing the financial target; learning about the target's strengths and weaknesses; planning to overcome financial crime controls; and fraud implementation.

The thesis proposed and tested the ALPi Model and identified variations between insider and outsider's deployment of tradecraft. Outsiders demonstrate greater levels of task intensity linked to access, learning and planning earlier in their fraud event timeline. Insiders demonstrate similar intensity, but later in their fraud event timeline; this suggests insiders and outsiders have different offending trajectories. Consequently, this finding led to a revision of the Time-allocation Model of Criminal Planning to reflect the post-crime activities of insider fraudsters (Allen, 2011). The thesis found outsiders deploy a greater variety of tradecraft than insiders who benefit from knowledge and access derived from occupational positions. Tradecraft aligned to access, learning and planning is classified and includes secondary

systems and organisational interface point access; learning through subversion and stigmergic processes; and the deployment of planned backstopping and operational security strategies.

The thesis defined three distinct learning periods common to all fraud event timelines. Pre-intent learning was generic, often linked to what was referred to as base line knowledge and access. Pre-crime and crime phase learning was targeted and deliberate, focussing on satisfying specific information deficiencies. Post-crime learning was reactive, disjointed, and focussed on the nature of actual or perceived threats. The thesis also identified the need to reframe routine activity theory's 'absence of capable guardianship' to a position that recognises a criminal's 'capability to overcome guardianship'. This acknowledges the role of individual agency in circumventing fraud controls by bringing the deployment of financial crime tradecraft into the fraud control narrative.

Finally, the thesis contended that until the complexity that is evident within the data is more fully understood, meaningful fraud prevention efforts remain bereft of their most important asset; that is, a detailed understanding of how fraudsters set about overcoming the controls that organisations seek to implement.

Abbreviations

AFP	Australian Federal Police
ALPi	Access, learning, and planning
AMEX	American Express
ANU	Australian National University
ATM	Automatic teller machine
AUSTRAC	Australian Transaction Reports and Analysis Centre
CSA	Crime script analysis
EFTPOS	Electronic funds transfer at point of sale
GST	Goods and services tax
IT	Information technologies
MDF	Main distribution frame
MICE	Money, Ideology, Coercion and Ego (Model)
NSWPF	New South Wales Police Force
NRL	National Rugby League
NSW	New South Wales
NSWPF	New South Wales Police Force
OIC	Officer in charge
OPSEC	Operational security
PIN	Personal identification number
PO	Post office
POS	Point of sale
SCP	Situation crime prevention
SOD	Separation of duties

Table of Contents

Candidate Declaration ..... **ii**
Acknowledgements ..... **iv**
Abstract ..... **v**
Abbreviations ..... **vii**
Table of Contents ..... **viii**
List of Figures ..... **xii**
List of Tables ..... **xiii**
Chapter 1: Introduction **1**
1.1 Financial Crime Control 3
1.2 Tradecraft and the Fraudster 6
1.3 Definition of Terms 8
1.3.1 Fraud 8
1.3.2 Tradecraft 11
1.3.3 Principal Fraudster 14
1.3.4 Insider 16
1.3.5 Outsider 16
1.3.6 Fraud Event Timeline 17
1.3.7 Temporal Activity Phase 18
1.3.8 Task Frequency 19
1.4 Research Gap 20
1.5 Research Aim 21
1.6 Thesis Statement 21
1.7 Research Questions 21
1.8 Research Scope and Approach 22
1.9 Thesis Structure 23
Chapter 2: Criminological Theories and the ALPi Model **27**
2.1 ALPi Model 27
2.2 Differential Association Theory 28
2.2.1 Criticisms 31
2.2.2 Learning 32
2.3 Strain Theory 35
2.3.1 Criticisms 39
2.3.2 Access and Learning 40
2.4 Rational Choice Theory 42
2.4.1 Criticisms 45
2.4.2 Planning 46
2.5 Routine Activity Theory 47
2.5.1 Criticisms 50
2.5.2 Access 50
2.6 ALPi Model and Criminological Theory 51
2.7 Summary 54
Chapter 3: Tradecraft **56**
3.1 Financial Crime Process Models 56

3.1.1 Fraud Triangle 57
3.1.2 Evolution of Financial Crime Procedural Models 66
3.2 Access 73
3.2.1 Routine Activities 73
3.2.2 Insiders 74
3.2.3 Outsiders 75
3.3 Learning 76
3.3.1 Métis and Techne 77
3.3.2 Criminal Learning Studies 79
3.4 Planning and Preparation 81
3.4.1 Offender Planning 82
3.4.2 Decision Making 84
3.4.3 Limiting the Chance of Detection 86
3.4.4 Evolution of Offending 86
3.4.5 Collaboration 87
3.4.6 Resources 89
3.5 Summary 90

Chapter 4: Methodology 93
4.1 Ethical Approvals 95
4.2 Qualitative Interviews 96
4.2.1 Semi-structured Interview Process 96
4.2.2 Data Collection 98
4.3 Secondary Data 99
4.3.1 Data Collection 99
4.3.2 Data Assessment 101
4.3.3 Data Management and Analysis 103
4.4 Summary 105

Chapter 5: Results 107
5.1 Case 01 107
5.2 Case 02 110
5.3 Case 03 112
5.4 Case 04 115
5.5 Case 05 118
5.6 Case 06 120
5.7 Case 07 123
5.8 Case 08 124
5.9 Case 09 127
5.10 Case 10 128
5.11 Case 11 131
5.12 Case 12 133
5.13 Case 13 135

Chapter 6: Tradecraft—Access in Financial Crimes 138
6.1 Access and the Insider 140
6.1.1 From Opportunistic to Planned 141
6.1.2 It's Part of 'My Job' 144
6.1.3 Crime and Collaboration 149
6.1.4 Conning Their Way in 151
6.2 Access and the Outsider 153
6.2.1 It's Part of 'Their Job' 156

6.2.2 Organisational Interface Points 162
6.2.3 Secondary Systems Access 166
6.2.4 Subverting Insiders 167
6.3 Summary 171

Chapter 7: Tradecraft—Learning in Financial Crimes 175
7.1 Learning and the Insider 176
7.1.1 Qualifications 179
7.1.2 Current and Previous Roles 182
7.1.3 Collaboration 185
7.1.4 Trial and Error 190
7.2 Learning and the Outsider 191
7.2.1 Qualifications 195
7.2.2 Current and Previous Roles 197
7.2.3 Collaboration 199
7.2.4 Criminal Facilitation 203
7.2.5 Trial and Error 204
7.2.6 Subverting Insiders 206
7.2.7 Research 209
7.2.8 Law Enforcement Products 211
7.3 Summary 212

Chapter 8: Tradecraft—Planning of Financial Crimes 215
8.1 Planning and the Insider 216
8.1.1 Planning Triggers 217
8.1.2 Temporal Planning Phases 222
8.1.3 Criminal Tradecraft 226
8.2 Planning and the Outsider 232
8.2.1 Planning Triggers 232
8.2.2 Temporal Planning Phases 237
8.2.3 Criminal Tradecraft 243
8.3 Summary 257

Chapter 9: Discussion 258
9.1 ALPi Model 259
9.1.1 Temporal Variation in the Implementation of Tradecraft 259
9.1.2 Revised Time Allocation Model of Criminal Planning 265
9.1.3 Revised Fraud Triangle 266
9.2 Tradecraft: Access in Financial Crimes 266
9.2.1 Access via Collusive Relationships 267
9.2.2 Access via Routine Daily Activities 269
9.2.3 Subversion 274
9.2.4 Intent 276
9.3 Tradecraft: Learning and Financial Crimes 276
9.3.1 Phases of Criminal Learning 277
9.3.2 Pre-intent Learning 278
9.3.3 Pre-crime Learning 279
9.3.4 Crime and Post-crime Learning 280
9.4 Tradecraft: Planning of Financial Crimes 280
9.4.1 Temporal Planning Phases 282
9.4.2 Planning Triggers 284
9.4.3 Criminal Tradecraft 285

9.5 Summary 286
Chapter 10: Conclusion 288
10.1 Limitations 289
10.2 Future Research 291
10.3 An Original Contribution to Knowledge 293
References 295
Appendices 313
Appendix A: Participant Selection Criteria 313
Appendix B: Participant Information Sheet 314
Appendix C: Written Consent Form 319
Appendix D: Letter to Participants 320
Appendix E: Interview Questions 321
Appendix F: Case Selection Criteria 324

List of Figures

Figure 1. Fraud event timeline 18
Figure 2. APLi framework 52
Figure 3. The fraud triangle 58
Figure 4. The fraud diamond 67
Figure 5. Fraud element triangle 69
Figure 6. The new fraud triangle 70
Figure 7. Revision of the fraud triangle 71
Figure 8. Simplified insider model (2018) 260
Figure 9. Simplified outsider model (2018) 261
Figure 10. Revised insider ALPi Model 262
Figure 11. Revised outsider ALPi Model 262
Figure 12. Revised fraud triangle 266
Figure 13. Routine activity theory revision 274

List of Tables

Table 1 *Early Process Models* 58
Table 2 *Studies Used to Explain How Fraud Occurs* 72
Table 3 *Data Coding* 100
Table 4 *Secondary Document Types* 101
Table 5 *Excluded Case Descriptions* 102
Table 6 *Selected Case Descriptions* 103
Table 7 *Case Status—Insider/Outsider Cases* 139
Table 8 *Insider Case Access Characteristics* 142
Table 9 *Outsider Case Access Characteristics* 155
Table 10 *Insider Case Data* 178
Table 11 *Learning Phases and Insiders' Criminogenic Knowledge Acquisition* 179
Table 12 *Outsider Case Data* 193
Table 13 *Learning Phases and Outsiders' Criminogenic Knowledge Acquisition* 195
Table 14 *Insider Planning Data* 217
Table 15 *Outsider Planning Data* 240
Table 16 *Data Synthesis: Access* 268
Table 17 *Data Synthesis: Learning* 278
Table 18 *Data Synthesis: Planning* 281

Chapter 1: Introduction

This thesis analyses the tradecraft of fraudsters with a focus on three criminal processes: access; preparatory learning; and planning. Focussing on access, learning, planning and implementation (ALPi) enables an analysis of variation in the implementation of tradecraft at the level of individual crimes, and improves understanding of how frauds are committed (Allan, 2018).[1] Observing crime at a micro level, this thesis assumes that a fraud involves a series of interconnected events rather than a one-off act (Cornish & Clarke, 1986; Ekblom & Tilley, 2000). This enables a more detailed analysis of fraudster tradecraft by highlighting variation in the timing of ALPi processes. The key variable in the operationalisation of a principal fraudster's tradecraft is their status as either an insider or an outsider. The significance of proximity to a target financial system is that numerous information demands must be met before the successful commission of the crime. Consequently, insiders and outsiders satisfy information demands in different ways.

The academic literature suggests that considerably less is known about how fraudsters commit their crimes, than why they do so (Allen, 2011; Benson & Chio, 2019; Braithwaite, 1985; Cornish, 1994; Levi, 1984; Morales, Gendron, & Guenin-Paracini, 2014; Suh, Sweeney, Linke, & Wall, 2020). Indeed, while Sutherland (1947, p. 6) suggested 'learning includes techniques of committing the crime', it remains the case that this focus has historically been overshadowed by scholarly works that prioritise motivations over actions (Matsueda, 1988). Therefore, this thesis deliberately places a greater emphasis on understanding how frauds are committed than on who fraudsters are, or why they commit a crime.

[1] ALPi predicts fraud will occur when a fraudster gains access to a system (A), learns how it operates (L), plans the crime (P), and implements (i) it in a way that lessens the chance of detection (ALPI).

This thesis makes two original contributions to the analysis of *how* fraud is committed. It proposes a new model of analysis and provides an exposition of fraud tradecraft. Additionally, the thesis proposes revisions to existing models and theories that address fraud. While criminology as an academic discipline has historically given preference to the analysis of motivations, fewer studies have focussed on the practical implementation of fraud (Albrecht, Turnbull, Zhang, & Skousen, 2010; Fathi, Ghani, Said, & Puspitasari, 2017; Gilmour, 2014; Haelterman, 2016; Hardy, Bell, & Allan, 2020; Lacoste & Trembley, 2003; Levi, 2008; Phillips, 2017; Suh et al., 2020; Wood & da Costa, 2015). Further, such studies tend to focus on a small number of similar frauds, which has the potential to limit the ability to generalise beyond specific crimes or settings.

The first key concept, the Access, Learning, Planning and implementation Model (ALPi Model) presupposes that for fraud to occur, the fraudster must gain access to the target financial system; learn how the system operates and how it has been designed to respond to illicit breaches; and finally plan and resource the fraud before its implementation (Allan, 2018, p. 38).[2] The ALPi Model explores these assumptions and provides a methodologically linked approach to the analysis of different fraud types. This thesis contributes to the defining and categorising of different types of tradecraft or skills observed in the commission of fraud. This provides researchers with the ability to delve deeper into the operationalisation of the cognitive strategies and techniques deployed by fraudsters during the commission of their crime, and their post-crime conduct. Also, drawing on the insight triggered by this thesis's focus on performance of a fraud, revisions are proposed to the time allocation model of crime planning (Allen, 2011), the fraud triangle (Wells, 1997) and routine activity theory (Cohen & Felson, 1979).

[2] This PhD candidature commenced in 2013. In 2018 the author of this thesis published a paper titled 'Insiders versus outsiders, alternative paths to criminogenic knowledge' which proposed the four components of the ALPI Model, without explicitly referring to it as such (Allan, 2018). While the foundation of this model remains the same, this thesis provides an updated version of the ALPi Model.

Finally, this thesis moves the current discourse on how fraudsters commit their crimes beyond a simple generalisation such as ‘it’s an insider crime’ or an ‘outsider crime’ to one that unpacks how the crimes were committed and why some fraudsters are successful in committing their crimes while others fail in their attempt. The value of this thesis is its novel focus on the ‘how’; the quality of the cases; and the fact that it draws these together with the observations of police practitioners tasked with investigating fraud.

1.1 Financial Crime Control

A limitation of modern fraud control discourse is its reliance on the use of a ‘one size fits all’ crime prevention approach across strikingly diverse settings. Generic modes of fraud prevention thinking advocate for increasing surveillance and fraud awareness training (Omar, Nawawi, Saiful, & Salin, 2016); fraud prevention policies and increased legal penalties (Prabowo, 2012); employee screening and audit committees (Schnatterly, 2003); and the tone and attitude of business leaders, to name a few (Laufer, 2011). Benjamin Franklin once proclaimed, ‘an ounce of prevention is better than a pound of cure’; 284 years on that adage remains highly relevant to the control of fraud (Butler & Raiborn, 2015; Chaikin, 2009; Franklin, 1736; Walsh, 2012). However, despite numerous controls being implemented across government, public and private sector institutions, the so-called ounce of prevention continues to fail to adequately live up to its potential because these crimes continue (Maulidi & Ansell, 2021; Omar et al., 2016; Seda & Tilt, 2020).

Notable Australian fraud cases including Ray Williams and HIH Insurance Ltd, Craig Thompson and the Health Services Union, Alan Bond and WA Inc and Christopher Skase and Qintex Ltd, are but a few examples of fraud control failures that persistently plague Australian businesses (McFarlane, 2001; Silver, 2013; Soheila, Ali, & Damien, 2005). However, rather than being committed in the proverbial Wild West, these crimes occur in highly regulated sectors permeated with levels of oversight and control considered at the time

to be effective. Despite the application of fraud controls, hundreds of thousands of fraud control failures occur every year across Australia (Australian Competition and Consumer Commission, 2021; Smith, 2018). This highlights the necessity for this thesis to unpack how frauds occur to inform future fraud control approaches.

It can be argued that an organisation's or industry's fraud control approach is shaped by belief systems relating to why fraudsters commit a crime. Take for instance the view that fraud is the product of a rational choice made by the fraudster, based on an assessment of the expected utility gain weighted against the potential cost of that action (Cornish & Clarke, 1986). This view logically points to a fraud control approach designed to increase the potential cost of crime—or target hardening—which negates the expected utility gain for the fraudster (Kroneberg & Kalter, 2012). This link between how crime is explained and how crime is controlled is seen in political manifestos dominated by slogans such as getting 'tough on crime' and 'do the crime, face the time' (Yates, 2003). Alternatively, if fraud is viewed as the result of a structural imbalance in society—where some are unable to achieve socially desirable goals—then rectifying the structural imbalance via improved education, health and housing programs become the answer (Merton, 1938; Murphy & Robinson, 2008; Murphy & Dacin, 2011). In the political realm, such crime reduction initiatives are dominated by slogans including 'for the many, not the few' (Meloni, 2014; Sipsma et al., 2017; The Labour Party, 2019). The significance of this is that a limited understanding of how crimes are committed results in less effective fraud prevention approaches.

Limiting the implementation of fraud control strategies to those that match an organisational, industry or political view on why crimes occur is problematic. Rational choice theory, for instance, does not account for the unplanned or reactive offender or the criminal willing to serve a custodial sentence (Goldstraw-White, 2011; Lanier, Henry, & Anastasia, 2004). Similarly, strain theory fails to account for those who commit crime having achieved

all their socially desired goals.[3] Therefore, while controls informed by these theories provide some level of utility, their deterrent effect for all individuals is limited. Not everyone is put off by the potential for incarceration or chooses to offend even though they have not achieved socially prescribed goals. While current fraud prevention strategies such as those informed by routine activity theory have their strengths (Cohen & Felson, 1979)—particularly as situational crime prevention strategies derived from this approach are easily implemented and understood—relying on a 'one size fits all' approach to fraud control still offers opportunities or gaps in either the measures or the capability of guardianship.[4]

Another reason why a fraud control regime may be ineffective is that while it was designed to work in one setting, it is not always possible to guarantee it will work in another. As a hypothetical example, two near-identical financial service providers use the same industry-standard fraud control mechanisms; however, company A has a corporate culture of 'sales come first' which might lead to an increase in sales fraud, while company B has a corporate culture of 'compliance drives success'. The influence of situational differences—for example, in corporate culture— is likely to have a direct impact on the effectiveness of fraud controls (Button & Brooks, 2009; McGrath, 2020). Indeed, the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry identified numerous examples of corporate culture failings as a significant driver (Hayne, 2018). Therefore, the effectiveness of control mechanisms can be negatively impacted by situational variations in where and how they are deployed. The ALPi Model, however, is used to describe the impact of situational variation in the learning and implementation of a fraudster's tradecraft.

[3] For a closer examination of relative deprivation see Webber (2007).
[4] This study does not explicitly criticise Situation Crime Prevention (SCP). Rather the examination of a fraudster's tradecraft is likely to aid in refinement of fraud prevention strategies that are deployed as part of a SCP approach.

1.2 Tradecraft and the Fraudster

Examining the tradecraft of fraudsters who commit complicated, high-value, high-impact frauds provides an opportunity to better inform and guide the development of fraud prevention mechanisms. Key questions guiding this research are *'why are some criminals successful while others aren't'* and *'can an examination of fraudsters and their activities help reshape crime prevention theory to improve professional practice control responses?*' These questions are addressed via an analysis of fraudsters' tradecraft that emerges from data collected from interviews with detectives and a series of criminal case management files compiled by the Australian Federal Police (AFP) and the New South Wales Police Force (NSWPF).

This thesis defines financial crime tradecraft as the operationalisation of knowledge, skills, and techniques and resources towards the attainment of a specific criminal objective (Allan, 2018).[5] Tradecraft is also the ability to 'operate secretly in hostile environments without detection from law enforcers' (Kenney, 2010b, p. 911). However, tradecraft is more complex than mere planning and preparation, as it is shaped by differing distal and proximal influences including specialised and general knowledge coupled with the stories, experiences and intuition shared between like-minded criminals (Cornish, 1994; Gambetta, 2009; Kenney, 2010a). Tradecraft is also shaped by relatively simple concepts including managing criminal associates, resourcing, opportunity and access (Benson & Simpson, 2018; Ekblom & Tilley, 2000).

A challenge for this thesis is that tradecraft is situationally specific; that is, what a fraudster does in one setting may not be the same in another. One way this has been addressed in the past is via an examination of specific crime types using methods such as crime script analysis, which provides a detailed analysis of the steps involved in the

[5] Resources could be an external fence to on-sell stolen property, or a money laundering specialist.

implementation of a specific crime type (Choi, Lee, & Chun, 2017; Haelterman, 2016; Maluleke, Motseki, Mokwena, & Dlamini, 2021; Smith, 2013; Van Nguyen, 2021).[6] While useful for detailing the specific stages of offending linked to specific crimes, such approaches potentially limit the capacity to generalise those findings to other crimes. Additionally, focussing exclusively on a single fraud type limits the ability to contrast the implementation of tradecraft across different frauds. This presents the opportunity for this thesis to add to the literature via the development of an approach capable of drawing conclusions from a wider variety of frauds types.

Rather than approaching the analysis of crime from a legal or moral perspective, this thesis proposes a procedural approach—one that identifies and describes the presence of meta-stages common to all frauds. Setting aside crime script analysis, which concentrates on drawing findings from an analysis of similar behaviours (Choi et al., 2017; Cornish, 1993, 1994; Haelterman, 2016, p. 7), it is argued here that analysing a wider variety of financial crimes will be useful in both the analysis and prevention of frauds. To achieve this, the ALPi Model focusses on three distinct stages (access, learning and planning) found across the fraud event timeline leading to the commission of a fraud that have largely been overlooked in traditional criminological studies. Classifying these interrelated behaviours for analysis and identifying similarities and differences between them allows researchers to better discern how and why fraudsters make decisions and how they operationalise their crimes across diverse settings. This informs professional practice rather than relying on general theories as it produces a micro-level examination of crime that can explain how these processes of offending work, how they function, and how they interact with each other.

[6] Some of the more recent crime script analysis studies (CSA) that examined financial crimes included Choi et al. (2017) who focussed on voice phishing, Maluleke et al. (2021) on credit card fraud, Van Nguyen (2021) on computer fraud, Hutchings and Holt (2015) on stolen online data, Smith (2013) on public sector corruption and Haelterman (2016) who used CSA to assist businesses to protect their assets.

1.3 Definition of Terms

This thesis is built on some key assumptions. First, financial crime is a series of interconnected micro-level events, rather than a singular inevitable event (Cornish, 1994, p. 155; Ekblom & Tilley, 2000; Haelterman, 2016, p. 7). Second, the proximity of the principal fraudster to the target financial system has a measurable impact on the deployment of tradecraft and the intensity of criminal activity at distinct periods as learning and planning unfold. These concepts within the setting of this thesis have specific meanings and therefore require clarification to delineate them from how they have been applied in other studies.

1.3.1 Fraud

Securities offences, bid rigging and price fixing are white-collar offences often referred to as fraud (Smith, Button, Johnston, & Frimpong, 2011). Much like white-collar crime itself, a definition capable of encompassing all these behaviours continues to remain elusive (Allan, Kelly, & Stephenson, 2018; Baker & Faulkner, 2003; Smith, 2002). Various attempts have seen scholars frame fraud by concentrating on the social status of the offender (Pontell, Black, & Geis, 2013; Sutherland, 1949), the nature of the criminal act (Benson & Simpson, 2018; Geis & Edelhertz, 1972) and the nature of the victim (Rothschild & Thorne, 1976). The most common approach is behaviour focussed and produces some examples including ‘human endeavor, involving deception, purposeful intent, the intensity of desire, risk of apprehension [and] violation of trust’ (Ramamoorti & Olsen, 2007, p. 53), with the suggestion that fraud is as simple as ‘obtaining of goods and services by deception’ (Levi, 2011, p. 162). Jones and Tickner (2004, p. 6) asserted it is ‘any significant and deliberate misrepresentation of financial affairs for the benefit of the perpetrator, or others for whom the perpetrator is acting’, while Benson (1985, p. 597) argued ‘fraud involves a conscious attempt on the part of one or more persons to mislead others’.

The main challenge is the inability of a definition to encompass the entirety of the concept given that it 'embraces all the multifarious means which human ingenuity can devise, which are resorted to by one individual, to get an advantage over another by false representations' (Albrecht & Albrecht, 2004, p. 5). The potentially unlimited number of behaviours that could be called fraud prompted Albrecht and Albrecht (2004, p. 5) to assert that:

> No definite and invariable rule can be laid down as a general proposition in defining fraud, as it includes surprise, trickery, cunning and unfair ways which another is cheated. The only boundaries defining it are those which limit human knavery.

An alternative approach to the identification of a common set of behaviours is to consider the shapes in which frauds manifest themselves. As already discussed, the term 'fraud' is perhaps a clumsy term to describe a substantial range of often highly complex behaviours. The alternative approach is to view fraud as a hypernym. In this sense, in the same way as 'colour' is a hypernym of 'blue', 'fraud' is a hypernym of false representation, procurement fraud or even financial misstatements.

Colour, which is a representation of human visual perception bounded by colour categories, in this instance 'hue', 'chroma' and 'value' provides a reference point against which to classify something as a colour. Fraud as a hypernym similarly requires distinguishing characteristics; for instance, according to Benson and Simpson (2009);

1. must be the intention to deceive another
2. the situation in which the fraud takes place is often a legal setting
3. no requirement for the contact between the offender and victim unlike some other crimes
4. criminals' actions often have an air of lawfulness about them.

It is however safe to assume that not all the categories listed above need be present in every instance for a specific act or omission to be classified as a fraud. Take for instance the door-to-door sales fraudster. Here the deception occurs in any number of guises including unfair contracts or misleading advertising; therefore, point 1 above is present. The familiar setting of door-to-door sales means that this type of meeting does not on the face of it appear criminal; therefore point 2 above is also present in this case. Because the victim invites the fraudster into their home, the primary location within which the fraud is 'generally' initiated, point 3 above is not relevant in this case as there is a need for the fraudster and victim to meet. Finally, because the victim invites the fraudster into their home, and this is normal because the fraudster appears legitimate by offering a product in which the victim may be interested, point 4 above is present in this case.

The advantage of fraud as a hypernym is that it allows the inclusion of a range of behaviours that have may have historically been excluded. Take, for instance, Braithwaite's (1985, p. 19) assertion that welfare cheats should not be included in the definition of fraud. Levi (2011, p. 162) in a similar manner suggested fraud was the 'obtaining of goods and services by deception', which rules out the possibility of a fraud such as tax evasion as this is often committed not through an objective act, but rather via an omission to act.[7] The disadvantage of considering fraud as a hypernym is that without definitional tightness, there is a danger of overindulging the concept and failing to settle on something useful that bounds certain behaviours together.

Keeping in mind the above classification (1, deception; 2, obfuscation of the true nature of the deceptive behaviour; 3, no necessity for offender and victim to interact directly; and 4, an overt attempt to make the behaviour appear legitimate) there is one definition that

[7] Rather that criticism of these definitions, this serves to highlight the difficulty in formulating a definition that is neither to narrow or too broad.

meets the overt question that this thesis seeks to address; 'how' a fraud event occurs (Benson & Simpson, 2018). Edelhertz (1970, p. 3) suggested it is 'an illegal act or series of illegal acts committed by nonphysical means and by concealment or guile, to obtain money or property, to avoid the payment or loss of money or property, or to obtain business or personal advantage'. Such a definition has found favour among some as a definition for the crime and thus guides this thesis (Allan, Kelly, & Stephenson, 2016; Allan et al., 2018; Baker & Faulkner, 2003).

1.3.2 Tradecraft

Modus operandi has traditionally been used by researchers to express the physical act of implementing a crime, with crime script analysis a common method to elucidate the mechanics of specific crimes (Choi et al., 2017; Hardy et al., 2020; Maimon, Howell, Moloney, & Park, 2020; Maluleke et al., 2021; Smith, 2013). However, what works well for crime script analysis in determining the modus operandi of crimes is also a limitation when the intent is to identify a broader range of behaviours, given it is difficult to generalise the findings from one crime script analysis study to another crime area when the behaviours being examined are generally linked to only one form of offending. Therefore, while the analysis of similar crimes provides the potential for a richer understanding of such crime, it is more difficult to generalise. The alternative is to focus on the assumption that seemingly different crimes will have a combination of both similar and different 'mechanical/practical' actions—actions that are selected based on differing contextual influences. These actions are hereafter referred to as tradecraft.

The emotional, cognitive and physical practices directly related to the commission of a crime are to criminals what tradecraft is to the intelligence community (Kenney, 2010b). In the intelligence field, tradecraft 'is the "how" of intelligence, the sources and methods that make the collection and analysis of intelligence possible' (Northcott, 2018, p. 289). The

earliest records of MI5 tradecraft, which in 1909 was the United Kingdom's counter-espionage section of the Secret Service Bureau, outlined intelligence tradecraft as:

1. collecting information on other countries
2. preventing other countries from collecting information on your country
3. misleading other countries via the dissemination of incorrect data (Northcott, 2018, p. 291).

From a criminal's perspective, tradecraft is the intentional and deliberately planned operationalisation of all necessary knowledge, skills and expertise to effect an outcome broadly linked to illegal activity. In the terrorism field, 'militants that wish to plan and carry out terrorist operations require knowledge of covert tradecraft, the knowledge and skills needed to perform clandestine activities in hostile environments without detection from law enforcers' (Kenney, 2009, p. 10). Based on this, tradecraft in a financial crime setting is likely to include all tasks undertaken in areas linked to how the fraudster gains access; how they learn and acquire the knowledge needed to commit their crimes; how they plan and prepare for their crimes; and finally how they implement their crimes. In this manner, this thesis demonstrates that a fraudster's tradecraft mimics the overarching aims described by Northcott (2018), in that criminals:

1. acquire the necessary information on their intended target
2. limit the chance of detection through considered actions
3. mislead others via deception.[8]

Tradecraft has been described as the application of 'artistic skill, cunning, and ingenuity' to a criminal endeavour, and is argued to include all cognitive and physical

[8] *See* Northcott, C. (2018). MIS's Tradecraft Before the First World War. *International Journal of Intelligence and Counterintelligence*, 31:2, 289-311. Drawing on materials from the Bletchley Park museum of Second World War code breaking, as well as the 1908-1909 writings of James Edmonds, the head of War Office Directorate of Military Operations, which later became known as MI5, Northcott traced the evolution of security services operational practice. These operational practices and now referred to as intelligence services tradecraft have parallels with the tradecraft demonstrated by fraudsters.

activities undertaken within a definable criminal activity phase (Knowles, 1999, p. 445). Tradecraft describes how victims are identified and selected (Jacobs, 2010, p. 514); and how fraudsters 'defy detection, obfuscate illicit activity, and avoid detection' (Jacobs, 1996, p. 359), make decisions (Beauregard, Leclerc, & Lussier, 2012) and acquire criminogenic knowledge (Allan, 2018). Therefore, tradecraft is essen

tially a description of processes linked to the commission of an offence; as such, within the scope of this thesis, tradecraft is the operationalisation of all knowledge, skills and techniques towards the attainment of a specific criminal objective.

The specific nature of tradecraft deployed by fraudsters is directly influenced by situational factors unique to each target system. For instance, an insider with account authority who fraudulently withdraws funds may seek to distance themselves from the crime by secretly using another's passcode; while the outsider may coerce a vulnerable insider to knowingly use their passcode. In each instance the passcode is required and used, but the way this is operationalised varies. As such, tradecraft consists of situationally specific behaviours bound by individual and organisational constraints. The importance of this nuanced view of these practices to the thesis is that each fraudster has a unique set of tradecraft fashioned within different operational settings. However, this does not preclude the possibility of making broader generalisations about the nature of tradecraft and as such this thesis demonstrates that tradecraft is comprised of the following characteristics.

- Victim selection—identification and selection of suitable targets (Jacobs, 2010; Vandeviver, Van Daele, & Vander Beken, 2015; Walsh, 2014)
- Gap analysis—identification and acknowledgement of mission-critical skill and knowledge deficiencies (Brezina & Topalli, 2012; Lacoste & Trembley, 2003; Vandeviver et al., 2015)

- Skills and knowledge acquisition—identification and acquisition of necessary skills critical to the fulfilment of a criminal objective (Steinmetz, 2015; Topalli, Dickinson, & Jacques, 2020)
- Relationship management—management of operationally important relationships (Weerman, 2003)
- Resource procurement and management—satisfying physical, human and information resourcing needs (Ekblom & Tilley, 2000)
- Operational security (OPSEC)—limiting the opportunities for guardians to disrupt the criminal activity (Jacobs, 1996; Jaques & Reynald, 2011; Knowles, 1999; Rashid, 2016)
- Backstopping—preparation and implementation of tactics to legitimise the authenticity of a material fact represented by the criminal.[9]

1.3.3 Principal Fraudster

Descriptions of fraudsters are relatively common but at times tend to be one dimensional. Take, for instance, assertions that a fraudster is a predatory stranger (DeLiema, Deevy, Lusardi, & Mitchell, 2020); that they 'commit fraud in a business environment, usually without any physical force, and confer an illegal economic advantage for themselves and/or for their organisation' (Schuchter & Levi, 2015, p. 176); or is 'someone who is greedy and deceitful by nature' (Padgett, 2014, p. 96). Such descriptions paint the picture of an individual acting in isolation towards an illegal outcome; however, instances of fraudsters acting in isolation are claimed by some to be in the minority (Morales et al., 2014). Indeed, most cases examined in this thesis involved multiple fraudsters who undertook a variety of

[9] The concept of 'backstopping' was raised by several participants. As such, this concept will be introduced into the academic literature later in this thesis.

criminal roles, which presents an alternate perspective against which to frame a fraudster's role.

Different crimes pose different challenges to those seeking illegal gain and not every crime can be committed by a single actor; instead, multiple actors may be required (Morales et al., 2014). This underscores the unlikelihood that each fraudster will fit a profile as espoused by Padgett (2014) or Schuchter and Levi (2015). Instead, as is seen in any other organisational structure including organised crime, there is often an array of roles filled by different individuals. The most important role, this thesis suggests, is that of the principal fraudster—the lead instigator behind the crime and the driving force who pulls the collective strings of all others to achieve the intended illicit outcome. The principal fraudster by this measure is the leader and principal decision maker in the criminal enterprise. Goldstraw-White (2011) offered an insight into the behaviours of fraudsters classified as principal fraudsters within larger criminal enterprises. As the key planner, this actor is described as a sophisticated criminal who weighs options before making decisions on crime targets and how to commit the crimes. Conversely, the opportunity actor, most often acting alone, chooses to offend when the opportunity presents itself with little to no other planning or antecedent behaviour (Goldstraw-White, 2011). Bernard L. Madoff, for example, was the principal fraudster in the Ponzi Scheme uncovered in 2008; however, he was not the only individual operating within that criminal enterprise (Hardy et al., 2020; Lewis, 2013a, 2013b). The principal fraudster, therefore, is the criminal who oversees, directs, coerces and manages the activities of all players towards the aim of achieving a defined illegal outcome, the combination of which leads to the commission of a crime. It is the principal who uses connections to address skill and knowledge deficiencies to overcome access issues, while at the same time ensuring that all actions are taken in a way that minimises detection.

1.3.4 Insider

Insiders are generally, but not exclusively, skilled individuals working within organisations and possess, or those who can (learn) acquire the knowledge, skills and techniques needed to achieve a criminal outcome (Allan, 2018; Ortega, 2006, p. 24). According to Cressey (1950, p. 742), insiders hold positions of trust that allow them to satisfy non-disclosable problems; something the Australian Government (2016, p. ii) described as the 'person who uses insider knowledge or access to commit a malicious act to cause harm'.

Trust violators as insiders hold what Felson and Boba (2010) referred to as specialised access positions that are the most common characteristic among white-collar criminals; and research findings point to insider opportunities as the greatest determinant of who will commit white-collar crimes (Benson & Simpson, 2018; Weisburd, Wheeler, Waring, & Bode, 1991; Wheeler, Weisburd, & Bode, 1982; Wheeler, Weisburd, Waring, & Bode, 1988). Insiders come in many forms including full-time or casual employees, along with contractors and customers—any individual who is entitled to or capable of performing a relevant function that gives them access to critical information or a financial system. Insiders, however, are not always principal fraudsters. For example, in Case 04 in this thesis involving theft by a union employee, the principal fraudster was the most senior employee in a single victim organisation; while in Case 12, a bank employee was only an associate fraudster.[10]

1.3.5 Outsider

The criminal outsider operates externally to the victim organisation and the target financial system, undertaking fraudulent activities via a range of mediums including the use of public-facing organisational interfaces such as:

- call centres and finance application forms (Allan, 2018, p. 40),

[10] As will be explained in more detail in Chapter 4, each case that comprised the data upon which this thesis is based was given a unique identifier, C01-C23. Linked to each case were principal fraudsters (PF01), associate fraudsters (AF01), other witnesses or victims (OT01), and participants (N01).

- sales and billing (Goode & Lacey, 2011, p. 704),
- procurement processes (Rendon & Rendon, 2016), and
- taxation declarations (Levi, 2010b).

The criminal outsider also plans, prepares and directs the activities of other outsiders and insiders towards the attainment of a criminal outcome. Despite the absence of legitimate access to target financial systems via an occupational position or customer–client relationship, outsiders use alternative means, including recruitment of insiders. In Case 07, principal fraudster PF07—owner of an automotive services company—and her co-offender AF07b who worked for an organisation with a large vehicle fleet—were both outsiders who operated externally to the debt-factoring companies against which they committed their crimes.[11] Outsiders also leverage 'information from insiders within the victim organisation to facilitate their crimes' (Allan, 2018, p. 42). For example, AF12a in Case 12 and AF01a in Case 01 both provided insider information to the principal fraudster who was outside and unconnected to their organisations, to further their crimes.

1.3.6 Fraud Event Timeline

Crimes, according to Cornish (1994, p. 155) 'are events with a specific location in place and time. But the crime event itself is only one among many events which occur within the crime-commission process.' Therefore, an important question that needs to be addressed in any examination of financial crime is what is included and what is not. A fraud, like other crimes in which a degree of planning is evident, can be described as a series of legal and illegal micro events. In this thesis, and within the constraints of the ALPi Model (Allan, 2018), these micro events can include any action or thought

[11] Debt-factoring is used in the automotive smash repair industry to recover the costs of repairs from insurance companies on time. It works by shifting the burden of collection from the smash repairer to a specialised debt-factoring company who in turn recoups the debt from an insurance company in exchange for a percentage fee of the owed monies. Doing so means the smash repairer is more easily able to raise working capital to put back into the business. See Case 02 in Chapter 5.

that contributes to the crime. Indeed, this consideration is not restricted to pre-crime, given the likelihood of post-crime actions being undertaken to limit detection. Therefore, in this thesis, a 'fraud event timeline' may commence before the formation of initial criminal musings and continue to a point post-crime where the fraudster ceases to act in ways specifically designed to prevent detection.[12]

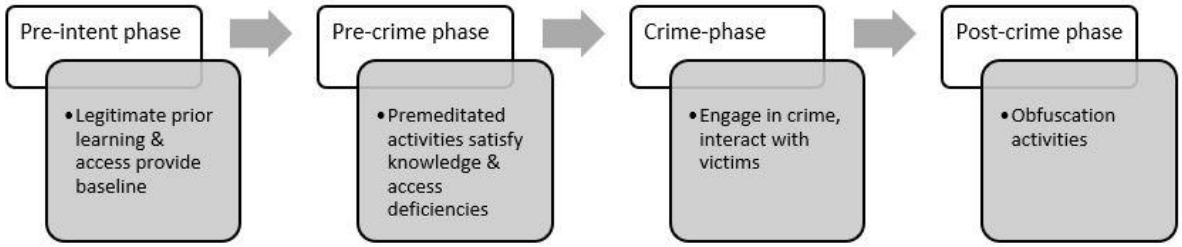


Figure 1. Fraud event timeline

1.3.7 Temporal Activity Phase

Based on the assumption that a fraud event timeline may commence at a point before the formation of initial criminal musings and conclude at a point at which the fraudster ceases to act in ways specifically designed to prevent detection, the fraudster will traverse a range of cognitive and behavioural states. This thesis broadens this concept of a temporal activity phase by describing it as a temporal theoretical construct that separates one cognition state from another. The first, pre-intent phase, describes the state where legitimate access and learning occurs before the formation of criminal intent.[13] The second, pre-crime phase covers temporal activities from after the formation of criminal intent until the crime is put into action. The crime phase is the next temporal element and covers all temporal activities associated with implementing the crime. Finally, the post-crime phase incorporates all

[12] It is not possible to identify a specific point in time when initial criminal musings might form, or a fraudster ceasing to act in a particular way are evident. However, this degree of boundary looseness allows the research to consider aspects of a criminal's behaviour that don't fall within a more definitive timeframe, for instance the implementation of the crime or the point at which the fraudsters profits from their crime.
[13] However, this is only where access or knowledge is directly relevant to the crime under examination.

activities following the implementation of the crime, up to the point in time where the fraudster ceases to take active steps to avoid detection.

1.3.8 Task Frequency

A key assumption of this thesis is the presence of variation in task frequency across the fraud process. 'Tasks' represent criminal activities including accessing victims, crime-specific learning, and planning and preparation; while the concept of 'frequency' acknowledges that certain points along the fraud event timeline will be busier than others. This position is supported by viewing crime not as a single point in time event, but as a series of micro events that, taken together, account for all activities that have a meaningful influence on the occurrence of crime (Cornish, 1993; 1994, p. 155; Cornish & Clarke, 1986; Haelterman, 2016, p. 7). Taken in its fullest sense, task frequency includes any cognitive or behavioural activity linked to the setup, execution and discontinuation of the crime, and can include:

- thinking
- planning
- reflecting
- deciding
- directing
- actioning
- constructing.

The fraud cases examined in this thesis are for the most part ventures of joint criminal enterprise. This requires different individuals to play various roles across the crime process (Morales et al., 2014). Logically, as each event commences there will be an associated increase in task frequency relative to the task. There are also periods of decreased task frequency during the crime process as timings, resources and people may not be available to

further advance the preparation of a crime on demand. Unlike a focus on geospatial criminal activity, as addressed by crime pattern theory (Brantingham & Brantingham, 1981, 1984), and temporal forms of analysis (Cohen & Felson, 1979; Hawley, 1950), task frequency in this thesis explains the volume and intensity of criminal activity undertaken at a specific point in time along the fraud event timeline while also identifying potential periods of inactivity. As these crimes are viewed as a series of micro events characterised by task frequency variation, observers can gain insights into periods of heightened criminal activity that highlight disruption opportunities from a police perspective, and become data points for researchers.

1.4 Research Gap

A fraud prevention strategy based on a 'one size fits all' philosophy fails to identify that while a series of crimes (e.g. procurement frauds) may be viewed from a legal perspective as the same, there will always exist nuances in how each fraud is committed. For instance, different fraudsters will arrive at their crimes with differing levels of access, knowledge and skills; consequently, their approaches to fraud will be subtly different. Additionally, the situational circumstances of one setting (e.g. a procurement department at a soft drinks company and a military procurement department) will undoubtedly be different in several ways. Such situational differences are likely to drive variation between these settings in the manifestation of the crime. As the mechanisms underpinning complex frauds and how they are committed are not fully understood (Allen, 2011; Benson & Chio, 2019; Braithwaite, 1985; Levi, 1984; Morales et al., 2014; Suh et al., 2020), it is necessary to address this limitation to develop or implement fraud prevention strategies more effectively (Pontell, 2009). Thus, a process analysis of features common to different frauds will aid in unpacking the subtle variation present across similar and different frauds to highlight opportunities for improved fraud prevention.

1.5 Research Aim

This thesis expands criminological understanding of how complex frauds are committed via an analysis of criminal case management files compiled by Australian police agencies between 2000 and 2012. Using the ALPi Model, this thesis provides a detailed account of the differences between insiders' and outsiders' approaches to access, learning and planning. In using the ALPi as a procedural model to understand fraudster behaviour, the thesis is built on an analysis of differential association theory (Sutherland, 1939), strain theory (Merton, 1938), rational choice theory (Becker, 1968) and routine activity theory (Cohen & Felson, 1979).

This model aids in identifying the influence of a fraudster's status as either an insider or an outsider to a specific crime target on how they deploy their tradecraft, as well as the cause of any differences between approaches. This thesis asserts that crime prevention strategies require a more nuanced understanding of how and why criminals identify criminal opportunities and implement their crimes to better identify and implement future fraud prevention strategies. This thesis aims to contribute the ALPi Model to the crime prevention discourse as a scalable and flexible method for identifying variation in the implementation of tradecraft, to more effectively guide future fraud prevention strategies.

1.6 Thesis Statement

It is hypothesised that a fraudster's status as either an insider or an outsider to a target financial system shapes how they deploy their tradecraft.

1.7 Research Questions

To provide a model with which to theorise common stages of offending, and identify differences in the deployment of tradecraft, this thesis specifically seeks to answer the following overarching research question, and subquestions:

1. To what extent are differences in the selection and deployment of tradecraft influenced by whether a fraudster is an insider or an outsider to the target financial system?
    a. How does access to financial systems differ between insider and outsider cases?
    b. How do learning and knowledge acquisition differ between insider and outsider cases?
    c. How do planning and preparation differ between insider and outsider cases?

1.8 Research Scope and Approach

The scope of this thesis is limited to an examination of fraud cases investigated by either the NSWPF Fraud Squad or the AFP Economic and Cyber Crime Directorate. Initially, a total of 23 cases was provided: 5 from the AFP and 18 from the NSWPF. However, 10 were excluded from the final data sample either because of a lack of supporting documentation or (as was the case with Cases 15 and 23) because they focussed on crimes outside the parameters established at the outset of this study.[14] [15]

The remaining dataset consisted of 13 completed criminal case management files, each augmented with a semi-structured interview with investigating detectives and open-source datasets to provide a qualitatively rich dataset. Reliance on data derived from crimes investigated by police agencies raises questions of data reliability, specifically in relation to criminals detected by police agencies. By that measure, these criminals were unsuccessful. Despite this, this thesis rejects the limiting concept of 'getting away with it' as an indicator of criminal success. Each case examined here resulted in funds being transferred from victim

[14] Case 16 / Case 17 / Case 18 / Case 19 / Case 20 / Case 21 / Case 22
[15] Case 15 was an investigation into a romance scam that targeted individuals, thus not meeting the requirements set within Appendix A. While Case 23 was an identity manufacturing investigation that had no connection to financial crimes and therefore did not meet the requirements set within Appendix A.

accounts into the control of the fraudsters. Additionally, the fraudsters were able to profit from most if not all of the proceeds they fraudulently obtained. Additionally, the crimes were in most instances different from each other regarding the systems they targeted, so much so that it is safe to suggest there were 13 completely different cases sampled. Ultimately, while this thesis is situated in an established field, it introduces and unpacks a relatively untouched area of criminology, specifically the tradecraft of fraudsters.

1.9 Thesis Structure

Chapter 2 introduces and describes the ALPi Model, which this thesis uses as its framework of analysis. The chapter then explores the four theoretical frameworks that underpin the assumptions driving the ALPi Model by drawing out relevant aspects from the original formulations of differential association theory (Sutherland, 1939), strain theory (Merton, 1938), rational choice theory (Becker, 1968) and routine activity theory (Cohen & Felson, 1979). The theories examined in this chapter 1) highlight the importance of criminal learning and the integral role it plays in financial crime, 2) identify the factors that shape criminal decision making, and 3) and examine the intersection of offender capability and criminal opportunity to establish differences in the implementation of tradecraft. This chapter argues that the examined theoretical frameworks drawn from criminology do not adequately account for how frauds are committed—specifically the tradecraft used in the commission of a financial crime.

Underpinned by the theories introduced in the previous chapter, Chapter 3 summarises findings from criminological studies that examined financial crime and led to the refinement of the underlying theories. It draws out aspects of these studies that begin to address the nature and shape of tradecraft. While this chapter notes an absence from the criminological literature of research exclusively addressing financial crime tradecraft, there exist across several studies insights into how fraudsters commit these crimes. These separate

insights are used to underpin the introduction of the ALPi Model along with its temporal and task-driven nature.

Chapter 4 describes the dual ethical approvals process and protocols implemented to ensure that the data were collected ethically and are credible. Because of the sensitive nature of the data, ethical approvals were sought from both the Australian National University and the two law enforcement agencies that contributed the data. The chapter describes the implications of the law enforcement approvals for this thesis, and the publishing restrictions placed on some of the data. In addition to detailed case analysis, the chapter describes the semi-structured interviews and secondary data collection undertaken and justifies the adoption of these methods.

Chapter 5 presents a synopsis of the data. Because of the sensitive nature of some cases, the potential risk of disclosing police investigative methodologies and third-party proprietary information, and the risk of inadvertent third-party identification, no detective transcripts, facts sheets, statements or any other case management data are included in this section. Consequently, all 13 cases are summarised and pertinent details presented to provide a comprehensive overview of each. Details summarised include case and detective identifiers, the jurisdiction of the crime and the offences committed by the fraudsters.

The analysis presented in Chapter 6 concerns the relationship between fraudsters and the target financial systems they seek to exploit. The key variable shaping this analysis is the principal fraudster's proximity to the financial system—specifically whether they are an insider or an outsider. Understanding the significance of this variable for different criminal enterprises helps to identify differences in the approach fraudsters adopt during the access stage of their crime. This analysis reveals the inherent connection between access and knowledge; in insider cases access occurs before the acquisition of knowledge, while in outsider cases, knowledge acquisition occurs before access. This highlights variation in

fraudulent offending patterns, and in doing so underlines the importance of access as a variable of analysis in the examination of complex frauds.

Chapter 7 examines the role of criminogenic knowledge in the crime commission process; specifically how, when and why it is acquired. Using four temporal reference points—pre-intent, pre-crime, crime phase and post-crime—this chapter identifies when insiders and outsiders satisfy information deficiencies. The chapter reveals that outsiders acquire most of the necessary systems knowledge in the pre-intent and pre-crime phases with little to no post-crime activities related to learning. In contrast, insiders demonstrated a more even distribution of learning-related activities across all four crime phases. Finally, this chapter provides a comparative analysis of the different means by which the insiders and outsiders satisfied their information needs.

Chapter 8 examines the planning and implementation stage of the ALPi Model as represented in the cases that make up this thesis. This chapter demonstrates that proximity has an impact on where the bulk of criminal activity (tasks) occurs along the fraud event timeline. For outsiders, a significant amount of planning occurs before the implementation of the crime with relatively little occurring post-crime. The operational criminal activity of insiders will tend towards the end of the fraud event timeline where they generally undertake a significant amount of planning to hide the crime from authorities, while at the same time distancing themselves from the crime. The difference is that the outsider seeks to access and exit the financial system with no one knowing who they were, even though getting into the system is harder for them than it is for the insider. In contrast, the insider criminal with easier access will have to work harder to obscure their connection with the criminal behaviour, because any subsequent investigation of crime may consider insiders with legitimate access to the financial system in the first instance.

Chapter 9 provides a coherent picture of the temporal nature of the ALPi Model's ability to reflect variation in how criminals commit their crimes. The chapter discusses the suitability of the ALPi Model as a framework for identifying differences between crimes. It contends that the proximity of the principal fraudster to the target financial system affects the micro-level stages of offending. Finally, the chapter addresses the implications of this thesis for the situational control of fraud and provides insights useful to those seeking new approaches to the identification of criminal activity surrounding the crime stages of access, learning, planning and finally implementation.

Finally, Chapter 10 draws this thesis to a close. It restates the intention of the thesis by reiterating the gap in understanding fraud tradecraft as identified in previous research. It restates the hypothesis that drove this and draws together the findings to provide an answer to the main research question. It reflects on the success of this research journey and identifies limitations of the study before offering insights into future research opportunities that have arisen from this thesis. Last, it restates the original contributions of this thesis to the field of criminology.

Chapter 2: Criminological Theories and the ALPi Model

This chapter draws on elements of criminological theory traditionally linked to the study of financial crime, specifically differential association theory (Sutherland, 1939), strain theory (Merton, 1938), rational choice theory (Becker, 1968) and routine activity theory (Cohen & Felson, 1979). However, this thesis is based on the premise that fraudsters are largely rational actors that undertake complex activities intending to gain financially through more efficient, albeit illegal, means. The complexity of these activities is captured by the processes covered by the ALPi Model and thus each stage of the model engages with different aspects of the four criminological theories examined in this chapter.

Each theory is analysed to identify whether it can account for how complex frauds are committed. While these theories are principally seen as explanations for why, not how, criminals commit their crimes, each offers a degree of utility in achieving this outcome. While they do not provide an account of the specific tradecraft practices displayed by fraudsters, each provides a starting point for further analysis. This chapter concludes by synthesising aspects from the four theories that relate to the ALPi Model, which has the objective of identifying how, rather than why frauds are committed.

2.1 ALPi Model

The ALPi Model is a process model that guided the development of this thesis (Allan, 2018, p. 38). The model enables analysis of differences in the process of applying tradecraft at the actor level; in doing so it improves understanding of how complex crimes are committed. The assumption underpinning the ALPi Model is that for fraudsters to commit complex frauds three related stages must be completed. Specifically, these are *access* to the financial system to acquire relevant and necessary *learning* including knowledge, skills and techniques, and finally *planning* and preparation for the crime before its implementation. Observing crime at a micro level, this thesis assumes that crime is a series of interconnected

events rather than a one-off event (Cornish & Clarke, 1986; Ekblom & Tilley, 2000). This view enables a more detailed analysis of fraudster tradecraft by highlighting variation in the timing of ALPi.

The ALPi Model is not a static framework of analysis; instead, it applies to the diversity of fraud seen today. For example, an individual without criminal intent becomes an employee of an organisation, thus gaining *access* to a financial system and *learning* how the system operates. Then, the employee forms a criminal intent, whereupon they *plan* and prepare for their crime. Finally, the employee implements their crime in a way that minimises their chance of detection. In another example, a fraudster who is not employed by the organisation acquires the necessary *learning*, then *plans* and prepares for the crime, gains *access* to the organisation or financial system and finally implements the crime in a way that minimises their chance of detection. In each of these examples, every stage of the ALPi Model was incorporated. However, in the first example the order is access > learn > plan; while in the second it is learn > plan > access. This, coupled with the logical assumption that fraudsters go through various iterations of access, learning and planning before the implementation of their crime, enables the model to be applied to any number of frauds so as not to exclude different crimes from analysis.[16] The utility of the ALPi Model also lends itself to an analysis of crimes other than fraud that require periods of planning before the event. This includes some terrorist events, hacking or even industrial/commercial sabotage.

2.2 Differential Association Theory

Differential association theory, as a general theory of crime, identifies learning as the main determinant of crime (Gottschalk, 2018; Lokanan, 2018). Sutherland (1933) proposed the presence of three interrelated concepts: normative (cultural) conflict, differential

[16] Initially included in the 2018 version of the ALPi Model (Allan, 2018), implementation has since had its importance to the overall criminal process minimised as it was observed that its inclusion simply repeated many aspects previously discussed in the access, learning and planning stages.

association and differential social organisation. The first of Sutherland's (1933) concepts, normative conflict, assumes society is segmented into groups that create conflict because of the existence of differences between the groups' norms, values and interests (Matsueda, 1988, p. 280). Tension arises when one group views a particular behaviour as morally repugnant, while a second views the behaviour as acceptable (Cressey, 1960, p. 48; Matsueda, 1988, p. 280). Therefore, crime can be a by-product of this cultural process where powerful social groups re-define certain behaviours as criminal (Matsueda, 1988, p. 281).

The second interrelated concept, differential association, contends that two processes occur at the level of the individual (Matsueda, 1988, p. 280). The first is the acquisition of skills and techniques to commit a crime (Sutherland, 1947; Sutherland & Cressey, 1974). The second—which Matsueda (1988, p. 281) suggested is more important as it explains why the individual commits a crime—is that the individual develops the specific drivers, motivations and rationalisations for committing a crime (Lokanan, 2018; McGrath, 2020; Sutherland, 1947; Sutherland & Cressey, 1974). In this manner, 'criminal behaviour is learned in interaction with persons via patterns of communication' (Cressey, 1960, p. 48; Sutherland, 1947, p. 6). This occurs as a result of normative conflict over what constitutes a crime (Matsueda, 1988, p. 281).

Set out in nine statements, Sutherland (1947, pp. 6-8) contended that:

1. Criminal behaviour is learned insofar as it is not an inherited trait.
2. It is learned in interaction with other persons in a process of communication.
3. The principal part of that learning occurs within intimate groups.
4. When criminal behaviour is learned, the learning includes
    a. techniques of committing the crime, which is sometimes very complicated, sometimes very simple
    b. the specific direction of motives, drivers, rationalization, and attitudes.

5. The specific direction of motives and drives is learned from definitions of the legal codes as favourable or unfavourable.
6. A person becomes delinquent because of an excess of definitions favourable to violation of law over definitions unfavourable to violation of the law.
7. Differential associations may vary in frequency, duration, priority, and intensity.
8. The process of learning criminal behaviour by association with criminal and anti-criminal patterns involves all the mechanisms that are involved in any other learning.
9. While criminal behaviour is an expression of general needs and values, it is not explained by those general needs and values since non-criminal behaviour is an expression of the same needs and values.

The final interrelated concept, differential social organisation, argues that crime rates are an expression of normative conflict (Matsueda, 1988, p. 282).[17] This argument contends that how societal groups are organised either in favour of, or against, law violation directly influences the rates of crime experienced within any setting, as crime is both entrenched in, and a by-product of, social disorganisation (Sutherland, 1947, p. 8). These groups, whether social, organisational, community or national are organised either for or against criminal behaviour, and as such 'crime is rooted in the social organization and is an expression of that social organization' (Sutherland, 1947, p. 8). Placing this discussion within an organisational setting, differential association theory provides a micro-sociological explanation of fraud via its acknowledgement of the 'link between individual actors and their immediate organisational circumstances' (Morales et al., 2014, p. 174). Finally, according to differential association theory, crime is a wilful violation of a set of laws promulgated by politically or

[17] Following Sutherlands death, Donald R Cressey sought to clarify some perceived confusion around cultural conflict and reframed it as normative conflict (Bernard, Snipes, & Gerould, 2016, p. 191).

socially powerful groups and applied to all members of society with breaches attracting proportionate penalties (Sutherland, 1947, p. 10; Sutherland & Cressey, 1974, p. 4).

2.2.1 Criticisms

Differential association theory is not without its critics (Burgess & Akers, 1966; Jensen, 1972; Kornhauser, 1963; Matsueda, 1982). Sutherland (1973, pp. 31-32), in an unusual self-critique, suggested 'the only thing needed to disprove a hypothesis is a single exception'; and then went on to offer two exceptions. The first is where despite exposure to excessive definitions in favour of law violation, if the individual does not have the opportunity to commit the crime, then the crime will not occur (Sutherland, 1973, pp. 34-37).[18] The second exception, the presence of alternative behaviours, entails instances where lawful alternatives exist concurrently with the criminal option (Sutherland, 1973, pp. 34-37). This negates the need to commit the crime by nullifying the premise that excess definitions always result in crime (Matsueda, 1988, p. 283). Additionally, the theory fails to account for instances of sudden, irrational or unexpectedly violent crimes in relatively benign settings; for instance, those where associations favour neither crime nor abstaining from crime (Kornhauser, 1963; Renzetti, Curran, & Carr, 2003).

As a theory of crime that relies on learning, differential association theory oversimplifies the learning process by neglecting to address the specific social conditions that are necessary and how skills and attitudes function as enablers of action (Kornhauser, 1963; McLaughlin & Muncie, 2006). For example, it suggests that criminal learning 'involves all the mechanisms that are involved in any other learning', which unhelpfully conflates the many ways in which learning is known to occur (Sutherland, 1947, pp. 6,7). For instance, behaviourist approaches advocate for repetition and practice (Skinner, 1931, 1938);

[18] This opening, initially cited by Sutherland (1949), provided a foundation for the later work by Benson and Simpson (2009) which advocated the importance of opportunity within the crime commission process. Which in turn was one of the early drivers for this thesis.

connective approaches advocate for collaboration and networking (Siemens, 2004); and cognitivism suggests learning is an internal process (Ginsberg & Opper, 1988; Piaget, 1980). Thus, Sutherland's (1947, p. 6) oversimplification undermines the principle that learning is done 'in interaction with other persons in a process of communication', 'within intimate… groups' given that not all modern learning theories agree on social sources as the only way individuals learn (Siemens, 2004). However, perhaps the most common criticism of differential association theory is that it is untestable (Cressey, 1960, p. 284; Gibbs, 1987, p. 827; Glueck, 1956, p. 99; Matsueda, 1988, p. 284). Matsueda (1988, p. 285) was sceptical of the above assertions when suggesting theories generally consist of a series of related propositions and theories are not effectively tested as a result. However, he acknowledged the difficulty of adequately proposing and formulating a mathematical formula capable of measuring certain aspects of this theory—most notably the ratio of definitions favourable and unfavourable to crime (Matsueda, 1988).

2.2.2 Learning

In its original formulation, differential association theory explained why crime occurs, and this focus on crime as a learned behaviour remains relevant to the contemporary examination of fraud (Lokanan, 2018; McGrath, 2020). Yet, despite Sutherland's extensive collection of works, the theory never transitioned to a generalisable explanation of how white-collar crimes are committed. Indeed, even proponents of differential association theory have gone so far as to relegate the importance of learning how crimes are committed (Matsueda, 1988, p. 281).

Suggestions that the learning of criminal techniques are less relevant than the learning of criminal motivations appear counterintuitive, as knowing how to commit a crime is of critical importance to the successful outcome of the crime (Hataley, 2020; Turner, 2020). Indeed, without knowing how complex financial systems operate, and having awareness of

one's inherent strengths and weaknesses, or one's own capacity to conceive criminal strategies to overcome system controls, it matters not whether the fraudster is motivated at a particular time. Simply put, in the absence of the necessary knowledge and skills, the success of any criminal endeavour is not assured. Therefore, any examination of how complex frauds are committed must include how fraudsters identify, satisfy and manage information deficiencies (Komesar, 1973).

Sutherland's (1947, p. 6) fourth statement, that 'learning includes techniques of committing the crime, which are sometimes very complicated, sometimes very simple', has not only been downplayed in the criminological literature but has historically been overshadowed by scholarly works that prioritise motivations over actions (Matsueda, 1988). For example, views including '[h]umans are social blanks until socialized' (Lanier et al., 2004, p. 149), and further arguments—such as that crime and criminality are not by-products of evil people; rather are learned much like anything someone learns throughout their life course (Akers & Jensen, 2007, p. 257)—highlight the imbalance in the focus between the learning of motivations over skills.

Differential association theory is driven by both individualistic and collective assumptions; specifically, the criminal acquires knowledge in social settings through interaction with others. Indeed, Sutherland (1924, p. 86) contended that knowledge is 'secured best by the individual case study'. In later studies, Sutherland (1947) proposed the concept of criminal maturity and contended it arises independently of physical and psychological maturity. Criminal maturity suggests people mature within their environmental and social settings; therefore the individual exposed to criminal patterns earlier in life will reach criminal maturity earlier than will one exposed later in life (Sutherland, 1947, pp. 199-200). Logically, as maturity evolves, the criminal increasingly considers how to commit the crime as well as how to do so in a manner that reduces the risk of detection—a point

addressed by Bennett and Wright (1984) in their examination of career burglars. In this sense, there is an important distinction to be made between criminal maturity and biological maturity and this provides researchers examining how complex frauds are committed with an opportunity to examine the criminal background of fraudsters to establish a causal link between criminal maturity and professionalism in criminal planning, preparation and implementation.

Designing a model to conduct a process analysis of complex frauds to address the research questions guiding this thesis relies upon first understanding how crimes are committed. Differential association theory provides a starting point via its contribution to the acknowledgement of the role of techniques in the crime commission process. Identifying the importance of technical skills and knowledge, and acknowledging that without opportunity a crime cannot be committed highlights the necessity of knowledge, skills and expertise to any process analysis of complex frauds (Allen, 2011).

Consequently, a process model needs to be flexible to account for variables likely to shape the learning process, including the point at which criminal intent forms. When intent forms before learning, it follows that learning is likely to be task directed and limited; whereas learning that occurs before the formation of criminal intent will be broader and more holistic. Therefore, several questions arise that need to be answered to assist with addressing the overarching research questions guiding this thesis:

1. How do fraudsters identify, satisfy and manage information deficiencies (Komesar, 1973)?
2. To what extent are information needs satisfied via occupational settings (Sutherland, 1939)?
3. What impact does the timing in the formation of criminal intent have on approaches to learning (Kenney, 2010a)?

2.3 Strain Theory

Deviance and crime allow individuals to identify behaviours that do not conform to societal norms, while at the same time legitimising the standards and expectations of the greater portion of society; that is, the conformists (Durkheim, 1982; Merton, 1968). As such, crime is a social phenomenon shaped by a range of processes and structures present within society (Bernard et al., 2016). In this manner, crime acts as a social indicator of broader social conditions, standards and attitudes (Henry & Einstadter, 2006). Crime is also more prevalent in sections of society with proportionately fewer legitimate opportunities to achieve prescribed goals via the use of institutionally prescribed means, which according to Merton (1968, p. 195) accounts for proportionately higher levels of crime in some socially deprived communities.

Strain theory arose from the concept of anomie or a sense of normlessness as initially proposed in 1893 by Emile Durkheim. Formulised following the industrial revolution, anomie suggested that when faced with changing societal values, individuals become uncertain and struggle in an apparent absence of societal guidance (Zembroski, 2011). However, while Durkheim's research focussed exclusively on increasing rates of suicide or deviance, crime was later linked to increases in anomie (Bernard et al., 2016, p. 128; Durkheim, 1952). Thus, the work of Durkheim set the foundation for structural–functionalist perspectives on crime (Zembroski, 2011). Merton (1938) conceived strain theory as a refinement to the normlessness of anomie. While anomie was a breakdown in societal standards and a failure to regulate natural human appetites (Bernard et al., 2016, p. 162), strain theory concluded that the interaction between culture or 'social structure' is the source of both appetites and a means of satisfying those appetites (Merton, 1938, p. 672).

The first social structure is the presence of culturally defined goals, or purposes and interests, which society presents as legitimate objectives worthy of pursuit by all members of

society (Merton, 1938, p. 672). Initially citing Mayo (1986, p. 158), Merton (1938, p. 674) identified monetary success, and later, the 'American Dream' (Merton, 1969, p. 260), as an element capable of producing anomie.[19] However, other than a slightly expanded discussion questioning the social consequence of the pursuit of wealth in a society not properly adapted for such a focus, Merton (1938) did not overtly repeat this connection. Nonetheless, ongoing discourse in this area has maintained the position that the pursuit of wealth remains central to his concept of 'culturally defined goals, purposes, and interests' (Merton, 1968, p. 189; Messner & Rosenfeld, 2013).

The idea of the American Dream has become synonymous with Merton's concept of culturally defined goals, purposes and interests, with Messner and Rosenfeld (2013, p. 6) arguing it refers to a 'broad cultural ethos that entails a commitment to the goal of material success'. Since then, the American Dream (or its counterpart in other societies) has remained central to the measurement of success in contemporary society because of its association with enabling self-worth, personal value and success (Bernard et al., 2016; Kubrin, Stucky, & Krohn, 2009; Murphy & Robinson, 2008). The second social structure, socially acceptable standards, 'defines, regulates, and controls the acceptable modes of achieving' the American Dream (Merton, 1938, p. 672). These standards are 'institutionalized, legitimate means (e.g., work)' and when coupled with education point to the appropriate way in which those embracing the American Dream should behave (Robinson & Rogers, 2018, p. 73).

If individuals embrace both the culturally defined goals and the socially accepted standards of achieving those goals, they are likely to be viewed and view themselves as successful members of society. However, where they embrace culturally defined goals yet lack the institutionalised means of achieving those goals, they experience strain (Robinson &

[19] Merton (1938) actually cited Mayo (1933); however the author of this thesis was unable to obtain the earlier version to confirm the reference to monetary success as a motivating factor. Subsequently, a later edition of the Mayo (1986) text was relied upon.

Rogers, 2018, p. 73). While institutional mores limit such behaviours, the alternative options including excessive use of force, deception and other deviant behaviours exist and are enticing to those inclined to achieve the American Dream in the shortest possible time (Merton, 1938, p. 675).

Merton (1938, p. 677) identified five ways in which individuals adapt to the strain created by the gap between their goals and their current state. Characterised by the acceptance of both cultural goals and institutionalised means, the first adaptation was identified as conformist; these individuals make up the largest portion of society. The significance of this adaptation being the largest portion of society is that through its numbers it establishes a set of common standards and expectations. In this way, it authenticates specific societal goals and modes of achieving them. Without these common goals and standards, social stability would not exist (Merton, 1968).

The second adaptation, innovation, describes the individual who pursues the cultural goals, yet strives to achieve them in a proscribed manner (Merton, 1968, p. 195). In this instance, the individual either rejects outright or fails to adhere to institutionally defined means of attaining the culturally defined goals. Examples include the use of fraudulent or corrupt practices to acquire wealth and the American Dream. The third adaptation, ritualism, rejects the idea of an all-out pursuit of socially defined goals associated with wealth and the American Dream (Merton, 1968, p. 203). Instead, these individuals scale back their aspirations of social mobility to the point where their lowered expectations can be more easily met (Merton, 1968, pp. 203-204). Despite this rejection, the ritualistic individual rigidly sticks to institutionalised norms.

The fourth adaptation, retreatism, rejects both the socially defined goals of the American Dream and the institutionalised means of achieving those goals (Merton, 1968, p. 207). This individual constitutes the smallest portion of society and is represented by the

vagabond; the chronic drunk or drug user; essentially the individual who, while viewed as existing ‘within society’, is effectively isolated from society either because of their own choice or because of extreme isolation. The fifth and final adaptation, rebellion, represents the individual who rejects both the culturally defined goals and the institutionalised means (Merton, 1968, p. 209). However, in this instance, the rebel seeks to replace culturally defined goals and institutionalised means with alternative goals and means of achieving them. Typically, groups linked with such an adaptation are ‘hippies’, and those who denounce the cultural standard of achieving the American Dream and instead opt to pursue alternatives choices.

Individuals, however, are not restricted to a single adaptation classification. Societal and economic conditions shift and exert pressure on individuals, resulting in temporal movement between adaptations (Cloward & Ohlin, 1970; Merton, 1968, p. 194; Murphy & Robinson, 2008). Contributing a sixth adaptation, Murphy and Robinson (2008, p. 511) proposed the maximiser as ‘one who utilizes both legitimate and illegitimate means in pursuit of the American Dream’. Combining conformity and innovation, the maximiser accepts culturally defined goals and institutionally prescribed means of achieving them, while at the same time using institutionally rejected means to achieve culturally defined goals. This blend of legal and illegal behaviours is evident in a range of high-profile white-collar crimes, including the Ponzi Scheme perpetrated by Bernard L. Madoff (Hardy et al., 2020), and the collapses of ENRON (Wood & da Costa, 2015) and HIH Insurance (Soheila et al., 2005). In all these cases, the principal fraudsters rose to positions of power and influence in multi-million-dollar organisations and were perceived to have achieved the so-called American Dream via institutionally prescribed means until their crimes were uncovered. Once this occurred it was evident that these individuals had also adopted more efficient, yet institutionally rejected means, in their pursuit of success. Thus, the maximiser type, as an

adaptation to strain, is strongly associated with crimes carried out within business settings, and thus within the constraints of this thesis is relevant to an analysis of how financial crimes are committed.

2.3.1 Criticisms

Strain theory has been subjected to criticism (Antonaccio, Smith, & Gostjev, 2015; Kornhauser, 1978; Langton & Piquero, 2007). Central to the argument initially posed by Merton (1938) is the assumption of one socially inclusive and defined goal that all members of society strive to achieve. This is counterintuitive as it is unlikely everyone can achieve this in the same way at the same time, and once some have achieved the initial target, further goals are likely to be set. Lemert (1964) questioned the authenticity of this position by suggesting strain is instead the product of an individual struggling to conform to a variety of standards prescribed by several different, often competing, groups within society. The oversimplification presented by the idea of one commonly defined aspirational goal ignores the agency of members of society who possess the capacity to both shape their perceptions and reject those imposed by others (Young, 1981). Therefore, relative deprivation is the result of a 'judgement that one is worse off compared to some standards accompanied by feelings of anger and resentment' (Smith, Pettigrew, Pippin, & Bialosiewicz, 2012, p. 203). In a similar vein, the assertion that there exists uniform pressure across all levels of society has been criticised (Kornhauser, 1978; Langton & Piquero, 2007, p. 1). Henry and Einstadter (2006, p. 175) identified strain theory's 'underlying assumption that structural conditions determine' an individual's response as shaping agency, while Murphy and Robinson (2008, p. 511) contended that without a measure of individual autonomy, some crimes—particularly frauds—could not occur without the individual being capable of pursuing alternative knowledge, skills and ultimately goals.

Another criticism facing strain theory is its tendency to oversimplify class analysis. Adopting a logic-based argument, Kornhauser (1963) suggested that as Merton and other prominent strain theorists claim lower social classes are weakly, rather than differently, socialised (Henry & Einstadter, 2006, p. 174), it is implausible that these classes all strive to conform with societally defined goals and abide by institutionally prescribed means. In a similar vein, an oversimplification of official statistics used by strain theorists to assert higher levels of crime in lower social classes neglects the significance of immoral, yet un-criminalised activities undertaken by members of the middle and upper classes (Henry & Einstadter, 2006; Pontell et al., 2013). Other criticisms of strain theory include the inherent difficulty of testing it objectively and the lack of clarity of what constitutes unlawful behaviour (Henry & Einstadter, 2006).

As a response to these many criticisms, strain theory was refined with the introduction of general strain theory (Agnew, 1992). This approach contended that rather than tying strain to a social structure source, it should instead be tied to a psychological reaction to any negative socio-psychological aspect present within an individual's environment (Langton & Piquero, 2007). This modification led to claims that general strain theory could explain all crimes (Agnew, 1992). It achieved this contested status via the introduction of three causal explanations for a crime:

1. failure to achieve positively valued goals
2. the removal of positively valued stimuli
3. the presentation of negative or noxious stimuli (Langton & Piquero, 2007, p. 2).

2.3.2 Access and Learning

Strain theory as it was originally configured addresses causal rather than procedural conditions. Therefore, it does not contribute to an analysis of how frauds are committed as it neglects the actual process of a crime beyond the point of the innovator (deviant) adapting to

societal strain. Surprisingly, insofar as the adaptations are concerned, Merton (1938) failed to address what crimes are committed, how they are committed, how fraudsters learn beyond the acquisition of cultural values, or even how success is achieved. Despite this, the combination of conformity and innovation goes some way towards describing how fraudsters gain the necessary access and knowledge to commit a complex fraud (Murphy & Robinson, 2008).

Like differential association, strain theory presents crime as shaped by its environment. There is an assumption that humans are social blanks at birth and then evolve via a process of socialisation, to develop rationality and learn socially defined goals in addition to proscribed behaviours, all within social settings (Empey & Stafford, 1991; Henry & Einstadter, 2006). Consequently, the innovator must learn the relevant skills and techniques, in addition to having the requisite opportunities to commit a crime, which highlights the potential blending of adaptations (Murphy & Robinson, 2008, p. 510).

The maximiser adaptation introduced by Murphy and Robinson (2008, p. 508) involves the simultaneous combination of conformity and innovation or legitimate and illegitimate opportunities through occupational roles. As such, this adaptation is useful in the examination of how crimes are committed through the blending of conformity and innovation towards illicit wealth acquisition (Tay, Puah, Brahmana, & Malek, 2016). Such a blend is seen regularly across a range of modern global financial crimes including ENRON and HIH Insurance, both of which saw seemingly respectable and high-profile figures abuse their occupational roles to commit crimes (Soheila et al., 2005; Wood & da Costa, 2015).

Fundamentally, the evolution of the maximiser adaptation accounts for the commission of crime across organisational settings. However, it also provides useful insights into aspects of the procedural steps that fraudsters take during the crime commission process. It identifies the blending of insiders' access and knowledge with illicit behaviours and

attitudes towards the implementation of crime. This indicates that consideration is given to factors including access opportunities; knowledge of financial systems; the realisable value within a system and associated controls; and that these are critical to the success of a criminal endeavour. Therefore, the maximiser adaptation provides evidence for the importance of access and knowledge in an examination of how complex frauds are committed. Thus, several questions arise that need to be addressed:

- To what extent does legitimate access arise from occupational positions (Murphy & Dacin, 2011)?
- To what extent do occupational positions satisfy all access requirements (Murphy & Robinson, 2008)?
- What factors influence the degree of conformity and innovation in fraud crimes (Murphy & Robinson, 2008)?

2.4 Rational Choice Theory

Originating from early economic and utilitarian explanations for decision making, rational choice theory assumes that rationality is directed towards the maximisation of economic returns (Becker, 1962, p. 1).[20] Therefore, from this perspective, crime is advantageous when the gain will be greater than the cost should the crime be detected (Becker, 1968, p. 170; Cornish & Clarke, 1986). As a theory, rational choice places autonomous choice at the centre of crime explanations (Crawford & Evans, 2012). Indeed, it rejects theories based on underlying biological, anomie, psychological and inherited traits, and instead views the fraudster as rational— an individual who chooses to commit a crime to gain a utility advantage. Therefore, fraudsters make decisions based on the extent of what they know, what they can achieve and the time they have available to achieve it (McLaughlin

[20] Becker's (1962) essay dealt with irrational behaviour and economic theory; however, it did provide the grounding for later studies including those by Cornish and Clarke (1986).

& Muncie, 2006). Accordingly, this approach contends that fraudsters 'evaluate the expected utility of both criminal and noncriminal activities and then choose the alternative with the highest net payoff' (Carroll & Weaver, 1986, p. 20).

Choice as a concept is far from straightforward. Fraudsters consider the ease of access to victims, the likelihood of getting caught and the potential for reward should the crime be committed (Allen, 2011, p. 28; Bernard et al., 2016, p. 47). Additionally, they also consider how costs and benefits can be altered, specifically increasing their gains and lowering their costs, while at the same time lowering the gains and increasing the costs for financial system guardians such as police agencies (Bernard et al., 2016, p. 47; Komesar, 1973, pp. 306-307). In a critique, de Jonge (2012, p. 9) contended that rationality is influenced by three premises:

1. limited resources to achieve an outcome, making it critically important to identify and utilise the most appropriate resources
2. the ability to make the most efficient use of those scarce resources
3. the efficient allocation of resources in a way that provides the greatest levels of utility.

Choice is influenced by a combination of experiences, memory, perceptions, beliefs and preference-ordering processes that shape learning via reflection (Kolb, 2014; Komesar, 1973, p. 307; McFadden, 2001, p. 355). As information, reflective experiences and memories are compiled over time, and the fraudster develops a cognitive repertoire that enables them to generate alternative courses of action from which to draw (de Jonge, 2012, p. 8). Influenced by a variety of 'financial, legal, social, physical and emotional restrictions' fraudsters then preference order the alternative options and arrive at the most preferable course of action (de Jonge, 2012, p. 8). Having done so, the fraudster is deemed a rational actor, assuming their chosen course of action is the most efficient means of achieving their desired outcome.

The efficiency of decision making is contested, however, as the process itself generates time and energy costs for fraudsters (Allen, 2011, pp. 28, 40; de Jonge, 2012, p. 9).

The collection, assessment and analysis of all available information, coupled with ongoing monitoring of evolving information sources, creates costs in terms of effort, potentially far greater than the expected benefit derived from knowing all the relevant information (Simon, 1978, p. 10). Indeed, the notion of weighing up the sum of all available information and possible alternatives suggests fraudsters are unlikely to ever achieve true rationality because of the impossibility of acquiring, storing and processing all information at the same time. Indeed, Carroll and Weaver (1986, pp. 20-21) contended that 'human rationality is seriously limited by biological constraints', which suggests that fraudsters are not able to take in all information and reduces the ability to make fully rational decisions. Additionally, studies in decision making (See, Einhorn & Hogarth, 1981; Slovic, Fischhoff, & Lichtenstein, 1977) have revealed an inability to make decisions in line with normative rationality: 'instead [people] make simplifications and shortcuts that are reasonable but may produce inferior outcomes' (Carroll & Weaver, 1986, p. 21). In this way, when deciding what course of action to take, fraudsters keep seeking alternatives until they are satisfied that they have enough information to make an informed decision, or until they get to the point of saying, 'enough is enough'. This means that decision making should be seen as getting to a point of being 'good enough' rather than perfect, considering available information, time pressures and the availability of scarce resources (Henry & Einstadter, 2006, p. 57; Simon, 1978, p. 10). Consequently, arguments levelled against normative views of rationality often centre on the inability to consider every possible alternative when making decisions (Boudon, 1998; Carroll & Weaver, 1986; Simon, 1978). Therefore, when coupled with preference-ordering processes, the additional decision costs directly influence the quality of the decisions made, as those costs potentially outweigh the perceived benefit associated with a chosen course of criminal action (de Jonge, 2012, p. 10).

Fraudsters are goal directed and purposeful, rather than senseless actors (Cornish & Clarke, 2006, p. 59). Goldstraw-White (2011) identified individual fraudsters who, as part of their criminal planning and decision making, made it a priority to ascertain both likely sentence severity and location of incarceration before weighing up whether to commit their crime or to desist. However other theorists continue to move away from viewing rationality as a completely 'hard-nosed' utility decision-making process, to one that is influenced by a range of other, less obvious and more complex factors (Taylor, 2013, p. 2). Ultimately, the concept of rationality is problematic as people often make decisions before knowing every potential alternative course of action. As such, rationality should be viewed as limited (Clarke & Cornish, 1983, pp. 49-50; Lanier et al., 2004, p. 340).

2.4.1 Criticisms

When considering the application of rational choice theory to an examination of how complex frauds are committed, the theory stops short of providing an in-depth analysis of the planning and decision making that proceeds and follows fraudsters' decision making. Criticisms of rational choice theory include its reliance on the premise that every person is capable of rationality (White & Perrone, 2015), and that any approach to understanding decision making based on the fallacy of universal rationality would result in outcomes disconnected from reality (Zafirovski, 2018, p. 194). The problem is that there is no such thing as perfect rationality because of the impossibility of retaining all objective facts in one's mind while systematically working through them to arrive at a perfectly rational decision. Instead, the concept of bounded rationality was introduced to better explain the limited amount of information an individual can possess and simultaneously process (White & Perrone, 2015). Another criticism is that it ignores non-rational crimes—crimes of the insane, stupid youth and mentally unstable person—none of which, it may be argued, possess the same level of rational thought as other crimes and as such, reflect diminished levels of

criminal responsibility (White & Perrone, 2015). Further criticisms include the inability of the theory to explain fundamental structural divisions within society (White & Perrone, 2015), or to explore the motivations of those who commit a crime; it simply accepts that motivation is present and proposes there will always be people who will commit a crime if the situation presents itself (Bernard et al., 2016).

2.4.2 Planning

To better understand how complex frauds are committed it is necessary to focus research attention on decision making linked to target identification, planning and preparation before the commission of a crime. Of particular importance is addressing questions raised by Allen (2011, p. 28) who identified the importance of researching '[h]ow do criminals plan their crimes, and what impacts that planning?' Additionally, decisions made by insiders during the post-crime phase warrant examination as this phase is most likely to include efforts to distance the criminal from the crime.

Having identified information deficiencies, potential victims and or threats of detection, fraudsters then make decisions based on what they know, what they can achieve and the time they have available to achieve their goals (McLaughlin & Muncie, 2006). This process of identifying problems, making decisions, gathering further information and/or acting is akin to problem solving and is likely to continue unabated from the initial identification of a criminal opportunity until well after the crime has been committed. Consequently, decision making is embedded in the fabric of all financial crimes and the examination of how complex frauds are committed must include how and why fraudsters make decisions, while also considering the situational factors that influence such decisions.

Designing a model to conduct a process analysis of complex frauds requires consideration be given to the fraudster's decision making; specifically, decision making that directly correlates with the planning of the crimes themselves. Thus, three questions arise that

need to be answered to assist with addressing the overarching research questions guiding this thesis:

1. To what extent do fraudsters consider the likelihood of getting caught (Komesar, 1973)?
2. To what extent do fraudsters plan based upon the desire to hide or legitimise their activities (Komesar, 1973)?
3. What influences the planning undertaken by fraudsters (Allen, 2011)?

2.5 Routine Activity Theory

Routine activity theory addresses, to some extent, the general omission in criminological theory of how crimes are committed. Cohen and Felson (1979, p. 599) identified a convergence of motivated offenders, suitable targets and the absence of capable guardianship as the primary explanation for why, where and when a crime occurs. In this way, routine activity theory allows for the examination of how crime opportunities arise, rather than unnecessarily restricting the focus to criminal motivations.

The ebb and flow of daily routines move potential victims towards or away from criminals (Cohen & Felson, 1979, p. 588; Sutherland, 1973, pp. 31-32). The rate at which crime occurs is linked to structural changes in society. Since change includes any variation or shift in societal parameters—for example, rising or falling employment—this will likely produce fluctuations in opportunities. At the time of Cohen and Felson's (1979, p. 589) publication of routine activity theory the increased need for dual family incomes was resulting in residential properties being left unattended during daytime hours. This was reversed during the COVID-19 pandemic, where working from home meant workplaces were increasingly targeted in commercial burglaries (Brewer, 2020).

The first component of routine activity theory specifies the need for a motivated offender. The theory does not attempt to understand or explain motivation; rather it assumes

criminal inclination is present (Cohen & Felson, 1979, p. 589). Next, as change is constant across society, logically, there is a continual supply of motivated offenders who will engage in criminal opportunities (Marcum, 2009, p. 41; Obstfeld, Brown, & Carlile, 2019). However, a closer examination of routine activity theory's central ideas suggests the presence of 'structural conditions [that] motivate individuals to engage in crime', which tends to indicate that even though 'criminal inclination [is taken] as given', there was tacit acceptance by Cohen and Felson (1979, p. 589) that structural conditions account for criminal motivation.

The second component of routine activity theory is the need for a suitable victim, usually operationalised as an attractive target. A suitable victim includes any prospective target deemed vulnerable within a defined setting and can include otherwise suitably defensible individuals or property. Take, for example, the vehicle fitted with an engine immobiliser left sitting in a residential driveway with keys in the ignition (Marcum, 2009, p. 42). In this example, the guardianship provided by the engine immobiliser is negated, and an otherwise inaccessible victim becomes a suitable target. Drawing on Hawley's (1950) work on human ecological theory, Cohen and Felson (1979, pp. 589-590) identified temporal patterns as important indicators for understanding crime. The temporal components of interest are:

1. rhythm, the daily routines of individuals taking them from their home
2. tempo, the frequency of those rhythms
3. timing, the way different individuals' rhythms bring them together (Cohen & Felson, 1979, p. 590; Hawley, 1950).

This suggests that suitability is also influenced by a victim's spatial alignment, a point developed by Meier and Miethe (1993) who proposed that the suitability of a victim includes their availability or presence at a suitable time and space coinciding with the presence of a potential offender. Other factors proposed by Cohen and Felson (1979, p. 591) affecting

target suitability include the relative material and symbolic value attached to the target/victim, as well as more mundane factors including its size and how easy it is for the offender to move it.

Guardianship, the third component of routine activity theory, includes both a human and non-human presence that can deter criminal activity. For example, natural surveillance occurs spontaneously in most communities and provides a level of self-guardianship (Reppetto, 1974); the physical characteristics of the target also influence perceptions of target suitability (Cohen & Felson, 1979, p. 591). The presence of passers-by or a padlock on a gate can also affect an offender's capacity to carry out their crime (Cohen & Felson, 1979, p. 591). Indeed, while an absence of guardianship may facilitate 'direct contact predatory violations' (Cohen & Felson, 1979, p. 595), so too may the presence of lax or ineffective guardianship (Marcum, 2009, p. 42). Guardianship also arises in occupational settings. Employees who commit frauds against their employers, and customers or suppliers, benefit directly from occupationally derived access and expertise. Insider fraudsters are ideally placed to identify deficiencies in internal control systems and on occasion can override existing controls, thus rendering them incapable (Cohen & Felson, 1979, p. 595).

Fraudsters, in a good fit with rational choice theory, are free thinkers who make rational, albeit limited, decisions constrained by their capacity to manage all information that would assist in their decision-making process (Lanier et al., 2004, p. 93). Fundamentally, the routine activity approach provides no differentiation between criminals and non-criminals other than that one group has broken the law and the other has not. While routine activity theory seeks not to understand or even explain criminal motivation,[21] it nonetheless refers to 'structural conditions that motivate individuals to engage in crime' (Cohen & Felson, 1979, p.

[21] While Cohen and Felson (1979, p. 605) acknowledge the presence of motivation, they nonetheless downplayed its significance when seeking to describe the situational factors that brought about crime by suggesting 'without denying the importance of factors motivating offenders to engage in crime, we have focused specific attention upon violations themselves and the prerequisites for their occurrence'.

589). This frequently overlooked acknowledgement suggests that societal conditions provide not only the opportunity for crime, but also a reason for an individual seeking criminal opportunities. Finally, crime from the perspective of routine activity theory 'is defined by the legal code such that there is no crime without law' (Henry & Einstadter, 2006, pp. 59-60; Lanier et al., 2004, p. 93).

2.5.1 Criticisms

Routine activity theory is not without criticisms relating to victim blaming (Birkbeck & Lafree, 1993); failing to consider the nature or motivations of the offender (McLaughlin & Muncie, 2006); and failing to explain why some people in general commit a crime when others do not. Additionally, when applied to complex frauds, routine activity theory is unable to account for situations where guardianship remains both capable and non-capable at the same time. For example, financial institutions' financial controls prevent many fraudulent transactions every day (Johnston & Spencer, 2011), while at the same time other fraudulent transactions succeed in defrauding the same financial institutions. This incongruity in guardianship suggests the presence of other variables that directly determine whether system controls are capable or otherwise.

2.5.2 Access

Routine activity theory highlights the importance of opportunity in the financial crime process. Whether achieved through random encounters, daily work routines or deliberately engineered, access is critical. Access also introduces to the examination of complex frauds a key variable—that of the fraudster's proximity to the financial system. Proximity in this sense is represented by the insider, while the opposite is represented by the outsider. In either case, access to a financial system is necessary. Where it does not arise naturally, as in the case of the insider, access must be engineered in some way by the fraudster to implement the crime.

Any examination of fraud and how it works must consider how access occurs, particularly in situations where access is not available via an insider. Additionally, examining access and opportunity provides an insight into how crimes are most likely implemented by criminals; thus, routine activity theory has a place in understanding how frauds are committed. As such, three questions arise that complement the main research question of how fraud is committed:

1. How is victim suitability determined in insider and outsider cases (Cohen & Felson, 1979)?
2. In the absence of legitimate opportunities, how do outsiders acquire access (Carnegie Mellon University, 2012)?
3. What factors influence different approaches to access (Walton, 2006)?

2.6 ALPi Model and Criminological Theory

The theories unpacked in this chapter each provide a unique explanation for the conditions needed to be present for a crime to occur. Of those examined, differential association theory (Sutherland, 1939), strain theory (Merton, 1938) and rational choice theory (Becker, 1968) adopt an individualistic approach by placing the criminal at the centre of explanations for why crime occurs, while routine activity theory (Cohen & Felson, 1979) considers the role played by the victim as well as the absence of guardianship. Despite differences between these theories, all four occupy common ground in their attempts to explain why crime occurs, and their inability to describe how individual crimes are implemented by fraudsters. This restricted focus on why individuals commit a crime means each theory offers only a little in the way of advancing understanding of how frauds are committed in their entirety. Despite this, each offers a unique, albeit limited, contribution to understanding how crimes are committed, as identified in Figure 2. When brought together,

these unique aspects provide a logical framework through which to analyse how complex frauds are committed.

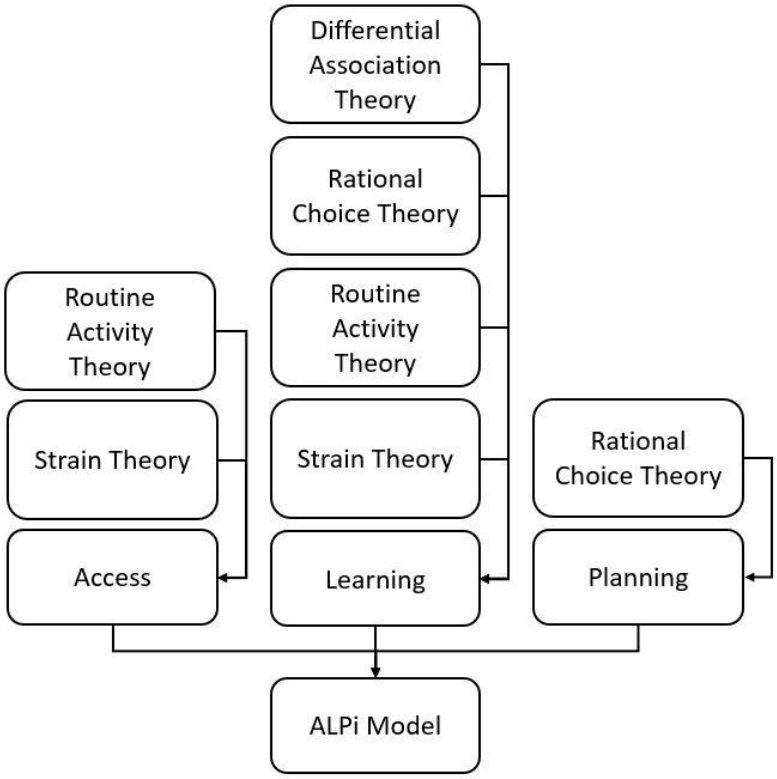


Figure 2. APLi framework

As identified in routine activity theory, strain theory and, to a lesser extent, differential association theory, a critical component in crime is access to a victim; in this case, the target financial system. The way this access occurs varies. As observed in Sutherland's (1939) differential association theory and Murphy and Robinson's (2008) maximiser adaption of Becker's (1968) strain theory, access is often generated through legitimate opportunities derived from employment and lawful access to financial systems. At other times, access is gained via illegal means including hacking or compromising internal systems via an agent or third-party insider (Wang, Gupta, & Rao, 2015). Additionally, the daily routine activities of a victim using the internet brings them into contact with observant fraudsters. In this sense, access can be enabled simply through the victim's presence online (Reyns, 2013).

Learning (knowledge/skills acquisition)—a critical component in any explanation of how fraud occurs—is referenced by all four theories. Knowledge is critical across the entire fraud event timeline: from victim selection to understanding a financial system's control function, pre-crime planning, overcoming information deficiencies, resourcing and learning from past mistakes are all essential to the successful outcome of a criminal enterprise. Like any endeavour, committing fraud requires knowledge, skills and expertise, and many of these information needs are satisfied via legitimate employment opportunities (Murphy & Robinson, 2008; Sutherland, 1939). Knowledge is also obtained via routine daily activities: for instance, career criminals pick up knowledge, skills and techniques from their normal criminal activities, essentially learning on the job (Cohen & Felson, 1979; Kenney, 2010a).

Planning is another critical component of complex frauds; however, of the four theories examined, only rational choice theory has the requisite explanatory power to illuminate how fraudsters approach the planning of their crimes (Becker, 1968; Cornish & Clarke, 1986). Setting aside the obvious question of why a fraudster commits fraud, and simply accepting that they have chosen to, a rational choice explanation provides a perspective on how fraudsters approach the planning of their crimes. Questions emerge relating to the planning undertaken before the crime, with consideration given to how fraudsters identify victims, information deficiencies, resource needs and the most efficient use of scarce resources.

As with all planned activities, unexpected events occur that require on-the-fly changes to original plans. Understanding how fraudsters respond to such events, identify new information deficiencies, satisfy those deficiencies and re-plan will help to better understand how complex crimes occur. Additionally, understanding the often-overlooked post-crime decision making and planning behaviours exhibited by fraudsters identifies the extent to which they actively seek to reduce their chances of detection during the immediate post-

crime period. Since the focus of this thesis is well beyond the one-off decision to offend, it is highly likely that decision making—and the corresponding planning—continues unabated from the initial identification of a criminal opportunity until well after the crime has been committed.

2.7 Summary

This chapter set out to establish whether four of the most cited criminological theories linked to fraud are able to provide a serviceable explanation of how such crimes are committed. The chapter analysed differential association theory, strain theory, rational choice theory and routine activity theory in their original formulations. Recent adaptations of these theories, along with criticisms levelled against them since their inception, were also examined, with the chapter concluding that while each purports to explain the reason for crime, they are unsuited to describing in detail how financial crimes are committed.

In drawing from the surveyed criminological theories, this chapter was able to identify the following overarching claim relating to how complex frauds are committed. That is, to commit a complex fraud, the fraudster must be able to access the target financial system and understand how the financial system operates to identify criminal opportunities. The fraudster must also be able to adequately plan and prepare their crime to overcome any internal controls linked to the financial system. Finally, the fraudster needs to be able to implement their crime in a manner that minimises their chance of detection by a capable guardian. Figure 2 shows how the analysed theories contribute to the ALPi Model in this thesis. The ALPi Model helps address a gap in the financial crime literature as it relates to limited numbers of studies exploring how financial crimes are committed (Braithwaite, 1985; Levi, 1984). From this point on, it is important to explore the extent to which empirical studies have focussed on the tradecraft practices deployed by fraudsters in the commission of their crimes. For this to be effective, the framework identified in this chapter is used to guide

the assessment of historical studies of complex financial crimes. Having established that the four theoretical frameworks examined in this chapter cannot individually explain how financial crimes are committed—but that through the collective, they validate each stage of the ALPi Model—the next chapter examines the extent to which the literature addresses the mechanics of the financial crime commission process.

Chapter 3: Tradecraft

This chapter analyses the financial crime literature to ascertain the extent to which studies have focussed primarily on questions of 'how' frauds are committed. The literature drawn upon was selected because of its links to the three stages of the ALPi Model. Although some of it focusses on frauds, other crime literature is drawn upon because of the inconsistent coverage of some areas of fraud in academic literature. The chapter begins by defining fraud and exploring models that describe stages of offending common to all frauds, to determine the extent to which existing criminological modelling accounts for the three stages of the ALPi Model (Cressey, 1953; Edelhertz, 1970; Kassem & Higson, 2012; Riemer, 1941; Wells, 1997; Wolfe & Hermanson, 2004). The analysis of this literature is aligned to each component of the ALPi Model. Finally, the chapter draws together the temporal stages of the three components into a comprehensive explanation of the ALPi Model.

3.1 Financial Crime Process Models

The conversion of criminological observations of trust violation behaviours into a process model is most often attributed to Cressey (1953). However, it was Riemer (1941, p. 411) who first identified the presence of three factors specifically linked to embezzlement:

- the social pull; the opportunity
- the social push; or 'emergency situation'
- the psycho-pathological element involved.

This approach theorised that opportunity is a causal factor since employees' or insiders' positions facilitate access to crime opportunities and knowledge that aids in avoiding detection. This early explanation of criminal behaviour described an emergency faced by the fraudster (Riemer, 1941, p. 414). Rather than viewing motivation as merely a get-rich-quick concept, motivation was triggered by the presence of a challenging situation such as extreme poverty, declining careers, pending bankruptcy or career instability. Other

factors, including the presence of psychopathological factors such as ‘difficulties adjusting to occupational life’ were presented (Riemer, 1941, p. 422). However, Cressey (1950) theorised that, rather than the psychopathic fraudster responding to life’s challenges, they can rationalise that behaviour to the point that it becomes acceptable. The key difference is that while Riemer (1941) viewed the offender as psychologically abnormal, Cressey (1950) viewed them as ‘normal’, or capable of justifying their behaviour to themselves to the point that they viewed it as morally acceptable. In this way, the foundations of the fraud triangle were established:

- a non-sharable problem
- an opportunity for trust violation
- a set of rationalisations that define the behaviour as appropriate in a given situation (Cressey, 1953).

Cressey’s (1953) work on rationalisation diverged only minimally from that of Riemer (1941), albeit rephrasing opportunity and the presence of a social push as a non-sharable problem. Thus, Cressey’s (1950) work is the leading framework for explaining fraud, and is second only to Sutherland’s (1947) differential association theory in identifying the conditions under which white-collar crime occurs (Schuchter & Levi, 2015).

3.1.1 Fraud Triangle

Wells (1997), drawing on Cressey’s (1953) work, coined the term ‘fraud triangle’. Although the phrase never featured in Cressey’s (1953) work, and Wells (1997) contributed both the model and the reframing of ‘non-sharable financial need’ to the more recognisable ‘pressure’ as seen in Figure 3 and Table 1, the latter’s contribution continues to be largely overlooked by contemporary scholars (Dellaportas, 2013; Huang, Lin, Chiu, & Yen, 2017).



Figure 3. The fraud triangle

Cressey (1950, p. 739) set out to establish the presence of specific variables during a crime and their absence during non-crime periods:

> The central problem of this study is that of providing an explanation in keeping with the assumption of proper scientific method and generalization by determining whether a definable sequence of events is always present when trust violation is present, and never present when trust violation is absent.

Meanwhile, Wells (1997) replaced the non-sharable problem with pressure, suggesting pressure occurs at some point during an embezzler's life course, but that it is not until the pressure becomes non-sharable that fraud occurs. When pressure builds, the individual takes action to relieve it, which leads to a lapse in morality (Morales et al., 2014, p. 178). Therefore, the original formulation of the non-sharable problem, with its range of plausible causal factors, provides a more versatile concept.

Table 1

Early Process Models

Reimmer (1941)	Cressey (1950)	Wells (1997)
Social push	Non-sharable problem	Pressure
Psycho-pathological element	Rationalisation	Rationalisation
Social pull	Opportunity	Opportunity

3.1.1.1 Pressure

Pressure is the most heavily scrutinised of the fraud triangle's three components (Benson, 2020). The sociological foundations upon which pressure builds or develops is influenced by societal norms and organisational expectations (Mills, 1940, pp. 909-910; Schuchter & Levi, 2015, p. 177). Indeed, contemporary mainstream theories including general strain theory (Langton & Piquero, 2007) and social learning theory (Akers & Sellers, 2011) identify the impact these pressures have on the formation of socially desired goals. Based on the hypothesis of the non-sharable problem, trust violators who are unable to address the non-sharable problem legally deal with it illegally and in private. Cressey (1953, p. 35) contended that 'not all trusted persons who have non-sharable problems become trust violators, but according to the theory here all trust violators have non-sharable problems'. The non-sharable problems or causal factors identified by Cressey (1953, pp. 36-57) are:

- violation of ascribed obligations
- problems resulting from personal failure
- business reversals
- physical isolation
- status gaining
- employer–employee relations.

Each non-sharable problem triggers a different type of strain, with shame and pride expressed by those unable to seek external support (Cressey, 1950). An inability to respond lawfully to non-sharable problems results in a breach of formal positions of occupational trust, and self-identified moral obligations to family and peers (Cressey, 1950). Along similar lines, multiple dilemmas of equal importance often arise and when individuals are incapable of managing these concurrently, they turn to illegal behaviours to satisfy one or more of these 'pressures' (Edelhertz, 1970).

Studies examining pressure as a causal influence have identified the so-called 'pressured actor', consisting of subgroups including the aspiring, desperate or threatened actors who respond to pressure (Goldstraw-White, 2011).[22] The 'desperate actor' (or business owner) facing loss commits a minor infraction to remain afloat and then commits increasingly more serious frauds to stave off ruin (Levi, 1981);[23] while the 'threatened actor' responds to external pressure such as a threat to loved ones, including the need to raise money for medical treatment (Peabody, 2001). In each situation, had pressure not arisen, had it been sharable, then the crime is unlikely to have occurred. There is, however, an alternative narcissistic explanation advanced as to why individuals commit a crime, and that is greed—a sense of superiority, ego challenge, power, benefiting the victim and group forces, all reasons commonly thought to motivate fraudsters (Stotland, 1977).[24]

Some studies have provided evidence of alternatives to the non-sharable problem hypothesis, including opportunity, greed, the threat of loss, superiority complexes, ego and power, benefiting the victim and group forces (Benson, 1985; Benson & Simpson, 2018; Smith et al., 2011; Stotland, 1977). Goldstraw-White (2011), for instance, identified the rational actor, a more deliberate and methodical individual. The rational actor can be divided into two sub-categories: planned and opportunistic. Planned actors demonstrate planned and calculating behaviours by weighing the potential benefits against the likely cost of detection. Indeed, some fraudsters investigate prison conditions and estimate the length of sentences imposed in similar cases to have a clearer understanding of the cons against which to weigh the pros (Goldstraw-White, 2011, p. 73). Therefore, planned actors are highly rational and

[22] Drawing on a series of interviews with convicted fraudsters, Goldstraw-White (2011) provided a comprehensive review of fraudsters motivations by exploring on fraudsters narrative which in turn provided insight into motivational and characteristic tendencies.

[23] In one perhaps one of the finest works in the financial crime space, Levi (1981) provided a comprehensive analysis of the long firm frauds, or planned bankruptcies.

[24] Stotland (1977, pp. 189-190) presented 'benefiting the victim' as akin to Madoff investors who reaped rewards for years prior to the collapse of Madoff Investment Securities LLC in 2008 whereafter they were ruined financially. Whereas 'group forces' represented the situation where fraud occurs as part of a business, however the fraud was 'not the main purpose of the business'.

methodical individuals who understand that crime can and does pay when they identify opportunities on which to capitalise.

3.1.1.2 Rationalisation

Rationalisation is the second element of the fraud triangle and focusses on excuses, denials and justifications (Maulidi, 2020). Rationalisation generally reduces internal conflict caused by contrasting feelings of right and wrong. For rationalisations of amoral/illegal contact to be successful, the fraudster must be exposed to, and internalise, cultural ideologies that align to and support their efforts to distance themselves from any illegality attached to their actions (Suh et al., 2020). This is achieved by altering their subconscious language to re-conceive embezzlement, for example as borrowing, as this helps normalise the behaviour and allows the fraudster to view themselves as law abiding; one who through no fault of their own found themselves in difficulty (Kassem & Higson, 2012).

The shape that rationalisation takes is contested. Sykes and Matza (1957, pp. 667-669), for instance, described 'denial of responsibility', 'denial of victim', 'denial of injury', 'condemnation of condemners' and 'appeal to higher authorities' as rationalisations, or techniques of neutralisation adopted by criminals. Meanwhile, Murphy and Dacin (2011, p. 601) contended that fraudsters arrive at crime by a variety of cognitive pathways, because of a 'lack of awareness, [or through] intuition coupled with rationalisation [and finally as the result of] reasoning'. In the case of reasoning, it has been suggested that crime occurs when the benefits outweigh the costs, which might explain how executives often regard their actions as a necessary part of their role, with its roots in cultural and environmental factors found within permissive organisations (Lokanan, 2018). Conversely, Free (2015, pp. 184-185) proposed 10 categories of rationalisation: moral justification; advantageous comparison; euphemistic labelling; ignoring or misconstruing consequences; denial of the victim; displacing responsibility; diffusing responsibility; entitlement; disbelief; and temporary loan.

Rationalisation is far from consistent as it varies by crime type. Anti-trust violators in the study of Benson (1985), for example, viewed their activities as aligned to industry practice, suggesting they were blameless as their actions were not for profit, but rather to avoid the burden of attracting additional work. They also ascribed predatory motives to regulators and contended their actions were not comparable to 'real' crimes such as robbery. Embezzlers, in contrast, acknowledged the criminality of their actions, while tax violators viewed their behaviours as merely the result of poor record keeping (Benson, 1985). Thus, anti-trust violators, embezzlers and tax violators all rationalised their crimes in uniquely different ways.

The direction of rationalisation also varies. Externally directed rationalisation lessens the perception of impact, such as 'it's a victimless crime' (Dellaportas, 2013); whereas internally directed rationalisations heighten personal needs, 'I wanted to improve my standard of living' (Suh et al., 2020). Consequently, fraudsters adopt different approaches to lessen their internal perceptions of criminality by either downplaying the impact of their actions or heightening the significance of their personal need. In either case, these perceptions attempt to align to acceptable moral codes of ethics (Albrecht, Hill, & Albrecht, 2006). Indeed 'offenders admit the wrongdoing but deny that it was wrong', which helps maintain a non-criminal view of themselves (Dellaportas, 2013, p. 32). This rationalisation of illegal behaviour overrides the presence of two contradictory cognition states—specifically, the acknowledgement of the illegality of the act and the self-held view of honesty—and as such this cognitive dissonance releases the fraudster to engage in illegal activities (Ramamoorti, 2008).

Rationalisation is also temporal: there are pre-crime rationalisations and post-crime justifications (Cressey, 1953; Sykes & Matza, 1957). Before the commission of a crime, it is not uncommon for criminals to engage in a form of cognitive preparation that enables the

denial of criminality (Dorminey, Fleming, Kranacher, & Riley, 2012). For instance, delinquents apply techniques of neutralisation before crime to release themselves from the obligation to comply with the law (Sykes & Matza, 1957). From a fraud perspective, the inclusion of rationalisation in the fraud triangle implies a degree of rationalisation is likely to be present pre-crime (Benson, 1985). Coupled with this is the image management exhibited by fraudsters (Wood & da Costa, 2015). Image management builds a perception of lawfulness, underscoring the presence of pre-crime rationalisations that permit crime (Stephenson-Burton, 1995), as well as preparing explanations or justifications for their actions should the crime be detected (Benson, 1985; Sykes & Matza, 1957). Therefore, the rhetorical question facing a fraudster would be, 'what can I do now that will aid me in achieving this state later?'

Following the act, offenders who had not previously considered their position, image or how others view their behaviour, are likely to give thought to or demonstrate activities that appear as post-crime justifications (Cressey, 1953). Justification enables offenders to distance themselves from labels of criminality (Morales et al., 2014; Sykes & Matza, 1957). The process of convincing themselves of their innocence reshapes their internal view of how their actions are perceived by others (Benson, 1985). This management of image by corporate elites is thought to allow them to deal with the impact of adverse publicity (Fisse & Braithwaite, 1983).

3.1.1.3 Opportunity

Opportunity, the final component of the fraud triangle arises 'when the fraudster sees a way to use their position of trust to solve the financial problem' (Kassem & Higson, 2012, p. 191). Initially described as social pull (Riemer, 1941), opportunity remains largely unchanged in the literature since its initial inception. In this formulation, it was described as the use of illegal shortcuts to accumulate wealth, including the abuse of positions of trust.

However, it also accounted for crimes in non-business settings where confidence tricksters create opportunities to target unwitting victims (Riemer, 1941).

Opportunity has received less attention than the 'non-sharable problem' and 'rationalisation' elements. Cressey (1973, pp. xii-xiii) doubted whether internal controls could eliminate opportunity, since 'modern business requires conditions of trust and that, therefore accounting controls rigid enough to eliminate embezzlement … will also eliminate business'. Such a focus on perception over actual opportunity places greater emphasis on the perceptions of organisational controls than on their effectiveness (Cressey, 1973). This suggests 'vulnerable environments [are] opportunistically interpretable scenarios' as some fraudsters are deterred while more skilled fraudsters find a way around the controls (Ramamoorti, 2008, p. 524). Therefore, while opportunities exist, they only do so for those skilled enough to identify and capitalise on them.

Historically, opportunity-focussed research has viewed fraud from the perspective of internal control failures (Lane et al., 2020; Lokanan, 2015). Alternative approaches have also focussed on the failure to punish or deter offenders (Roche, Wilson, & Pickett, 2019; Schell-Busey, Rorie, & Simpson, 2020); occupational positions as indicators of opportunity (Mohliver, 2018; Sohoni & Rorie, 2019); and the ability of management to override controls (Avortri & Agbanyo, 2020; Mohliver, 2018). While each view has access as a common element, the question that remains is what happens when the principal fraudster is an outsider?

Logic suggests that opportunity, as a component of the fraud triangle, should not be limited to occupational positions or happenstance encounters. Instead, opportunity can be deliberately engineered through actions designed to render otherwise adequate controls inadequate. Central to this is the importance of knowledge, skills and techniques in crime (Lokanan, 2015). While knowledge of 'assets, people, information, and computer systems

that enable [them] not only to commit the fraud but [also] to conceal it' might generally be obtained via employment situations, the same knowledge can be obtained by outsiders via alternative methods (Coenen, 2008, p. 12).

Opportunity is influenced by capability and resources. The fraudster that understands how a financial system is designed to detect fraudulent or illegal actions is better placed to minimise the chance of detection. This, it is suggested, accounts for instances in which what are normally effective controls are overcome by criminal expertise (Messerli, 2020). The so-called perfect crime—that of hiding embezzlement in previously settled expenditure—is enabled via competent knowledge and the ability to alter records (Riemer, 1941). To achieve the perfect crime, certain barriers must be overcome—first, using the requisite knowledge and skills; and second, via the ability to internally balance risk against reward. Ultimately, it is knowledge and expertise that make fraud possible within complex and protected business environments.

3.1.1.4 Criticism

Despite the fraud triangle's utility, it has been subject to criticism. Cressey (1950), for instance, avoided collaborative crimes that restricted the examination of frauds where the lack of criminal expertise in one fraudster is addressed through collaboration with another. Indeed, an individualistic focus only serves to heighten the focus on rationalisation and motivation at the expense of opportunity. Cressey (1953) was also sceptical of internal controls, which is ironic given that the fraud triangle is frequently used as a call to strengthen internal controls (Maulidi, 2020). Similarly, the fraud triangle fails to explain complex frauds where the violator had no trust to breach in the first place. Another weakness involves a reliance on the assumption that a motivated offender was also a capable offender. Since Cressey (1953) built his work on Sutherland's (1939) ideas, which were themselves premised on the learning of both techniques and rationalisations, the omission of capability alongside

motivation was an oversight. As a result of this, the fraud triangle continues to be both refined and expanded (Free, 2015; Kassem & Higson, 2012). While subsequent refinements, which are explored later in this chapter, addressed some of these criticisms (Kassem & Higson, 2012; Wolfe & Hermanson, 2004), this thesis contends that the successful modelling of financial crime must address not only capability but also its operationalisation if the aim is to understand how financial crimes are committed.

3.1.2 Evolution of Financial Crime Procedural Models

The fraud diamond is the most notable extension of the fraud triangle, with the introduction of capability (see Figure 4) (Wolfe & Hermanson, 2004). Capability addresses the fraud triangle's obvious weakness that without certain skills and expertise, some frauds will not occur (Free, 2015). Interestingly, capability is not classified as a single trait. Instead, it is dependent upon the setting in which the crime takes place. For instance, Wolfe and Hermanson (2004, p. 40) contended that capability included:

1. position/function
2. brains
3. confidence/ego
4. coercion skills
5. effective lying
6. immunity to stress.



Figure 4. The fraud diamond

Capability relies on a fraudster's knowledge of the financial system, because persons who repeatedly perform work functions develop specialised knowledge of how systems work (Wolfe & Hermanson, 2004). In this way, capability is linked to opportunity (Benson & Simpson, 2018), and across corporate settings, this is more likely to be found at management levels where increased knowledge, access and authority are coupled with lower levels of oversight (Yusof & Lai, 2014). However, this view fails to account for the capability of fraudsters who are external to the organisation and do not regularly perform relevant work functions.

Capability is not consistent across time and does not always exist before the formation of criminal intent. For instance, capability developed in a legitimate occupational position before the formation of criminal intent is different from capability gained after the formation of criminal intent. An example of the latter is a principal fraudster gaining access to an occupational position to acquire the necessary knowledge, skills and expertise. Similarly, the principal fraudster who collaborates with an insider achieves capability via another person, and after the formation of criminal intent. Indeed, a fraud may be committed in the complete absence of an authoritative occupational position; for example in the case of some hackers. Access, therefore, is key to both opportunity and capability, as access to occupational positions, and/or access to people or systems is a critical enabler.

Of the individual traits identified by Wolfe and Hermanson (2004, p. 40) the capacity to understand and exploit is the most important. However, this concept is far from simple when viewed from an educative perspective, as the transition from understanding to exploiting complex systems requires more than the recital of facts (Kolb, 2014). Instead, effective learning requires the operationalisation of knowledge through practice, reflection, refinement and repetition (Ginsberg & Opper, 1988). As such, the second trait, 'brains', must acknowledge the role of learning and planning as the process involved in understanding and exploiting is intertwined with the fraudster's capacity to acquire, process and successfully use complex information. This provides a more nuanced understanding of how capability manifests differently across frauds.

The value of exploring capability further is that while an opportunity may exist, or be sought, and incentive and rationalisation embolden the criminal, capability remains critical (Maulidi, 2020; Yusof & Lai, 2014). Omar et al. (2016, p. 1015) suggested that 'without capability, such as individual know-how, confidence, lying skills and manipulation of the situation, an individual may not commit or is incapable of committing fraud'.

The introduction of capability moved the thinking around the fraud triangle from the assumed position that mere opportunity results in crime, to one that indirectly acknowledges the influence of control mechanisms on crime and the need for deliberate criminal thought to overcome them. However, suggesting 'I have the necessary traits and abilities to be the right person [and] I can turn it into reality' precludes the idea that the fraudster lacking those skills can still execute the crime by engaging the services of others with the necessary skills, thus tackling a skills shortage via the expertise of others (Wolfe & Hermanson, 2004, p. 39).

Positioned alongside the fraud triangle as a cue to guide auditors in the investigation of fraud, the little-known 'fraud element triangle' describes how crimes are committed by fraudsters at a meta-level (see Figure 5) (Albrecht, Albrecht, Albrecht, & Zimbelman, 2006).

It achieves this by addressing the physical act of crime including the *Act*, specific methods deployed by fraudsters; the *Concealment*, efforts to hide the crime; and *Conversion*, how the fraudster converts the proceeds of crime to their use (Albrecht, Albrecht, et al., 2006, p. 84). The benefit of this is an ability to identify and document specific actions undertaken by the fraudster (Dorminey et al., 2012). It highlights distinct stages of the offending process and further moves the discourse beyond motivational debates. The weakness of this model is that it stops short of identifying the existence of obvious micro-procedural stages of offending as highlighted by the ALPi Model and crime script analysis approaches (Cornish, 1993).

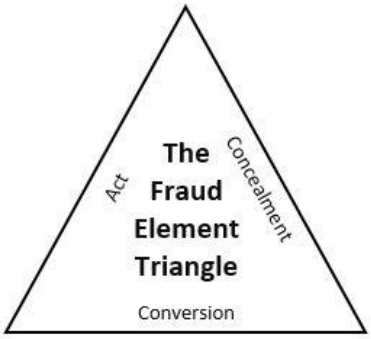


Figure 5. Fraud element triangle

Kranacher, Riley, and Wells (2011) furthered thinking around the fraud triangle by unpacking its motivational aspect with the Money, Ideology, Coercion and Ego (MICE) Model. Dorminey, Fleming, Kranacher, and Riley (2010, p. 21) contended that while the model oversimplifies fraudulent motivations, it provides an effective typology against which to classify motivational differences. Money or greed as a self-evident motivating factor was joined by ideology, the self-justification of committing a crime for the greater good as defined by prescribed belief systems; coercion, where the fraudster is unwillingly involved; and ego, which confronts a loss of reputation that can also lead the fraudster to commit a crime to avoid the loss of status (Kassem & Higson, 2012).

Kassem and Higson (2012) proposed the new fraud triangle (see Figure 6). Synthesising several models, their model claimed to increase an external auditor's knowledge

of how and why fraud occurs. Critical of the place of rationalisation and pressure in earlier models, as these factors are difficult to observe, Kassem and Higson (2012) argued for the replacement of *rationalisation* (Cressey, 1950) with *personal integrity* (Albrecht, Howe, & Romney, 1984); a nuanced return from incentive (Wolfe & Hermanson, 2004) to *motivation* (Kranacher et al., 2011); and the introduction of *capability* (Wolfe & Hermanson, 2004). Personal integrity, according to Albrecht et al. (1984, p. 18) is 'the code of ethical behaviour each person adopts' and is more readily understood because decisions and decision-making processes can be observed directly while rationalisation is less easy to observe (Kassem & Higson, 2012). However, an obvious weakness with the new fraud triangle is its apparent neglect of the procedural stages of offending that are imprecisely identified in Figure 5 (Albrecht, Albrecht, et al., 2006).



Figure 6. The new fraud triangle

Previous attempts at accounting for how frauds are committed have several deficiencies, specifically in the conceptual space that exists between opportunity and capability. These limitations include an inability to account for the capability shown by outsider fraudsters; assumptions that motivation and capability are synonymous; underplaying the necessity for skills, knowledge and techniques; and the necessity for the 'capacity to understand and exploit accounting systems and internal control weaknesses' (Wolfe & Hermanson, 2004, p. 40). To understand 'how' fraudsters commit their crimes it is

necessary to reframe the new fraud triangle into something more likely to provide a picture of what occurs in practice across a broader range of fraud cases.

Having analysed the relevant strengths and weaknesses of previous models that contributed to the new fraud triangle, the next step is to consider revisions that will help to explain how frauds occur. To achieve this outcome this thesis proposes a revision of the fraud triangle (see Figure 7), which switches *opportunity* and *capability*. This is because opportunity exists independently from capability and thus switching the two reflects the reality that capability must be brought to bear upon an opportunity situation. However, the question that remains is how is capability operationalised? No two crimes are the same given variation in the knowledge, skills and competencies of different offenders. Coupled with differences in financial systems, internal controls and organisational cultures strongly directed towards or away from unethical behaviours, any explanation must provide flexibility. Therefore, for any model to properly account for how frauds are committed, it must provide flexibility in its account of how fraudsters access financial systems; how they acquire the necessary knowledge, skills and techniques; and how they plan and prepare for a crime.

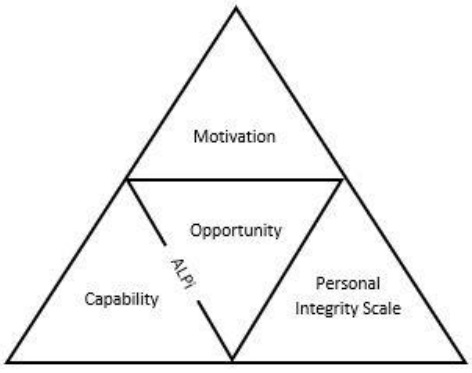


Figure 7. Revision of the fraud triangle

Conceptually, the placement of the ALPi Model at the intersection of opportunity and capability provides a necessary link between these two concepts and emphasises that the

commission of fraud is foremost an interdependent process, see Table 2. Rather than a rigid link, this offers a degree of flexibility to account for differences that arise between insider and outsider crimes. It offers greater granularity in the examination of the fraud event described by Albrecht, Albrecht, et al. (2006), as temporal elements of offending are not temporally fixed stages. Instead, they remain fluid and responsive to a variety of influences. Take, for instance, the insider who 'learns how [the financial system operates and] responds to unauthorised access, then, with criminal intent, plans their crime with that knowledge, finally implements the crime in a way they believe is least likely to result in their detection' (Allan, 2018, p. 38). In this instance, the temporal order is access > learn > plan > implement. However, consider the alternative of learn > plan > access > implement, as in the case of a hacker who learns a new technique in a dark web forum, plans the crime and then hacks the financial system (Zhang, Tsang, Yue, & Chau, 2015). It is also possible that these temporal elements occur more than once during a crime sequence, for instance where access is gained on multiple occasions, or where an unforeseen issue arises requiring further planning on the part of the fraudster.

Table 2

Studies Used to Explain How Fraud Occurs

Riemer (1941)	Cressey (1950)	Wells (1997)	Wolfe & Hermanson (2004)	Kassem & Higson (2012)	ALPi Model
Social push	Non-sharable problem	Pressure	Incentive	Motivation (MICE)	
Psycho-pathological element	Rationalisation	Rationalisation	Rationalisation	Personal Integrity	
Social pull (Opportunity)	Opportunity	Opportunity	Opportunity	Opportunity	Access Learning
			Capability	Capability	Planning

3.2 Access

Opportunity is central to almost all explanations of how crime occurs. This section examines *access*, the first element of the ALPi Model, and explores research that has sought to understand how criminals access their victims. Several studies are analysed to 1) confirm the validity of focussing on *access* as a temporal element in financial crime and 2) determine the extent to which *access* has been addressed in research.

Opportunity is '[a] time or condition favourable for a particular action or aim' (Stevenson, 2007, p. 2013); while access is '[t]he action or process of obtaining stored documents, data, etc' (Stevenson, 2007, p. 13). Therefore, an opportunity is the convergence in time and space of a combination of circumstances where an outcome becomes possible, while access transverses the possible to the actual. Framing it in another way, an opportunity is the potential to commit a crime, while access is the way entry is gained.

3.2.1 Routine Activities

The most frequently cited path to crime is through daily routine activities. Routine activity theory was developed at a time when homes became vacant during weekdays as both adults entered the workforce (Cohen & Felson, 1979). Data showed that burglars were taking advantage of opportunities by targeting households (suitable victims) when homeowners (capable guardians) went to work (Federal Bureau of Investigation, 1976). Such structural changes brought offenders and victims together in temporal spaces, thus heightening the opportunity for crime. Similarly, the advent of credit cards posted by banks to residential addresses brought motivated offenders into contact with unsupervised credit cards located in residential mail; thus routine daily activities provide both opportunity and access for the motivated offender. The inherent ease of access to financial systems by both insiders and outsiders satisfies *access* as the first temporal element of the ALPi Model, as without opportunity, access to a financial system—and ultimately the crime—will not occur.

3.2.2 Insiders

By virtue of their position, insiders have unrestricted access to their victims. Occupational positions bring criminals and victims together within organisational settings (Ortega, 2006), and in many situations, criminals hold what are known as specialised access positions (Australian Government, 2016). Such positions facilitate the acquisition of knowledge that, when coupled with access, enables the exploitation of vulnerabilities (Felson & Boba, 2010).

Broadly speaking, research has revealed three types of insider: the unintentional insider, the opportunistic insider and the malicious insider (Carnegie Mellon University, 2012; Goldstraw-White, 2011). Unintentional insiders mistakenly disclose valuable or sensitive information; for instance leaving classified information unattended in public (Kim & Nigel, 2008). The opportunistic insider, however, reacts to opportunities in workplaces by exploiting specialised access; for instance in the insurance industry following natural disasters (Pao, Tzeng, & Wang, 2014). Research also suggests that three-quarters of all fraudsters in Australia are classified as opportunistic offenders (Australian Government, 2016).[25]

Malicious insiders differ from unintentional and opportunist insiders as they actively seek opportunities. This insider seeks to compromise system integrity via abuse of trust to affect their criminal intention (Australian Government, 2016). There are three potential types of malicious insider: the insider seeking criminal opportunities within their organisation; the insider who is subverted by external actors; and the insider who seeks employment to commit a crime, something Sutherland (1941, p. 112) referred to when suggesting that some persons seek out organisational positions of trust, as they offer ‘opportunities for criminal behaviour

[25] Compiled by the Commonwealth Attorney-General’s Department, this study drew exclusively on information and case studies from the United Kingdom’s Centre for Protection of National Infrastructure. Additionally, data were drawn from the United States Federal Bureau of Investigation.

in relative secrecy and security'. The subversive insider, according to Walton (2006, p. 11), is active and generally relies on disillusionment, bribery, blackmail or ideology.

A subversion occurs during employment, either when the fraudster is already employed, or during the pre-employment phase in cases where they are seeking employment opportunities (Walton, 2006). Pre-employment subversion is potentially the greatest threat faced by organisations because the loyalty of the subverted insider is most firmly attached to the external entity (Walton, 2006).

3.2.3 Outsiders

Outsiders are thought to be involved in as many as 50% of insider cases (Centre for the Protection of National Infrustructure, 2013). In this thesis, the outsider is defined as the fraudster that operates externally to an organisation and undertakes fraudulent actions via a range of organisational interface points, including call centres and finance application forms (Selzer, 2006), sales and billing (Goode & Lacey, 2011), procurement processes (Rendon & Rendon, 2016) and taxation declarations (Levi, 2010b).

Despite a lack of access to organisational systems, outsiders plan, prepare and direct the activities of others (Carnegie Mellon University, 2012). Leveraging connections to satisfy information deficiencies and implement aspects of their crimes, outsiders often subvert insiders (McClymont, 2012). Instances of subversion are difficult to address from a control perspective as the insider's connection is often aligned in favour of the outsider rather than the organisation (Walton, 2006). From an information security perspective, outsiders pose the gravest threat to organisations as they damage financial systems and steal confidential information (Walton, 2006). A common feature of outsiders is their limited opportunity to carry out their attacks, primarily because of a lack of legitimate access, meaning their only avenue to crime is via the exploitation of weaknesses in crime controls (Walton, 2006). When

this is considered in the light of the fraudster attempting to exploit a weakness, then weakness is often a subverted insider.

3.3 Learning

Without knowledge of opportunities, without skills to undertake crime, crime cannot occur. This section examines *learning*, the second element of the ALPi Model, and the criminal learning literature. A series of studies are analysed to 1) confirm the validity of *learning* as a temporal element in financial crime and 2) determine the extent to which learning has been addressed in previous studies. Learning is the acquisition of 'knowledge of (a subject) or skill in (an art etc.) as a result of study, experience, or instruction' (Stevenson, 2007, p. 1569). From a criminal perspective, learning involves the same cognitive developmental processes as learning undertaken by legitimate workers in other settings (Dellaportas, 2013), with the exception of learning criminal motivation and rationalisation.

Crimes against financial systems require knowledge of structural opportunities. The acquisition of this knowledge generally occurs at one of two times. The first is via legitimate occupational roles (Cohen & Felson, 1979); for example 'knowledge and skills, gained either through previous employment experience' (Goldstraw-White, 2011, p. 76) or 'knowledge developed from the profession in which the offender is practiced gives rise to opportunities that allows offenders to recognise and exploit' (Dellaportas, 2013, p. 37). In most cases, individuals acquire that knowledge legitimately via employment, specifically before the formation of criminal intent. Such positions provide fraudsters with the opportunity to develop an understanding of how financial systems operate and their inherent vulnerabilities (Felson & Boba, 2010). In one of the earliest financial crime studies, Geis (1970, p. 175) noted some employees were indoctrinated into patterns of illegal behaviour in workplaces, with one research participant reporting '[m]y first actual experience was back in the 1930s, I

was taken there by my boss … to sit down and price a job' and '[i]t had become so common and gone on for so many years that I think we lost sight of the fact that it was illegal'.

The second method of satisfying information deficiencies occurs after the formation of criminal intent. Some fraudsters actively research specific systems or organisations (Goldstraw-White, 2011). Others source more generic information online via dark web forums (Lane et al., 2020), or use professional facilitators like accountants, lawyers, taxation consultants and real estate agents (Levi, Nelen, & Lankhorst, 2005). Fraudsters also subvert organisational insiders to satisfy information deficiencies (Carnegie Mellon University, 2012). The experienced insider provides information and access, while inexperienced insiders research relevant information to meet the needs of the outsider. Finally, studies have also identified offenders actively seeking positions of employment with organisations they intend to target in the future (Hutchings & Holt, 2015).

3.3.1 Métis and Techne

In an examination of terrorism events, Kenney (2010a, p. 178) suggested researchers must consider two types of operant knowledge: 'abstract technical knowledge' (techne) and 'practical, experiential knowledge' (métis).[26] Similarly, fraudsters must possess relevant knowledge to commit their crimes. Indeed, without knowing how complex financial systems operate, without an awareness of their vulnerabilities, or the ability to conceive criminal strategies to overcome control systems, it matters not whether a motivated offender has identified a suitable victim that lacks a capable guardianship (Cohen & Felson, 1979). Simply put, without the necessary knowledge, skills and techniques the success of any criminal endeavour is not assured.

[26] Drawing on fieldwork with Islamist militants in Britain and Spain, Kenney (2010a) examined the role of learning in Islamist settings.

To unpack capability, establishing how an offender's knowledge is developed is important. Techne, according to Kenney's (2010a) description, is acquired in many ways; for example, the accountant or lawyer develops technical knowledge via higher education. This is unsurprising as white-collar offenders are more likely to be university educated than are non-white-collar criminals, or the public (Ragatz, Fremouw, & Baker, 2012; Ruhland & Selzer, 2020). However, it is unwise to hypothesise an exclusive link between techne and university qualifications because the same data reveal that a portion of each sample is not university educated. Techne therefore can be sourced from other places, with the most obvious being on-the-job learning (Kembrey, 2016).

Techne for the outsider is likely to include the same learning opportunities as the insider; for example through university education and previous employment. However, the outsider may acquire techne from other sources. This is likely for several reasons. First, because techne is often situationally specific, the way organisations operate may differ, even within the same industry. Second, organisations evolve and the longer the offender remains an outsider the greater the reduction in techne currency. Therefore, the offender must satisfy deficiencies in other ways; for example by subverting insiders who provide specific systems knowledge, thus remedying the techne deficiency. Techne deficiencies can also be overcome in places like dark web hacker forums (Zhang et al., 2015).

Métis, conversely, is acquired through immersion, practice, reflection and refinement over time (Kenney, 2010a). Experiential and situational learning is more readily acquired via direct personal experiences or through interactions with others in proximal settings (Kolb, 2014). While it is possible to acquire métis via online settings, Kenney (2010a) was less certain of its overall effectiveness compared with informal and practice-based learning derived from direct personal experiences. Métis is also likely to arise in instances where repeat offenders learn from their mistakes. For example, when police seize the proceeds of

drugs sales, this sends stigmergic signals to criminal syndicates, identifying supply chain failures (Nieto-Gomez, 2016).[27] Such signals trigger first a process of initial flaw hunting to identify how police successfully intercept the proceeds of crime (de Jonge, 2012), and second a refinement of criminal processes to protect the criminal syndicate against future losses (Nieto-Gomez, 2016).

3.3.2 Criminal Learning Studies

There is variation in the breadth of research that focusses on criminal learning, with some studies referring to the 'learning criminal' (Hataley, 2020; Hutchings & Holt, 2015; Kemp, Zolghadriha, & Gill, 2019) and others addressing the diffusion of crime (Baker & Faulkner, 2003; Mohliver, 2018), all of which highlights the importance of learning to the crime commission process. The 'two types of diffusion of fraud' model proposed by Baker and Faulkner (2003) suggests criminal learning encompasses the identification of opportunities, the refinement of motives and justifications, and the exploration of relevant techniques. Accordingly, learning occurs in one of two ways: via social networks and via impersonal methods. Diffusion via social networks occurs when fraudsters share crime opportunities, techniques, motivations and justifications with each other (Jones, 2019). Financial crimes learned in social settings include benefit fraud where the learning is shared among family groups (Tunley, 2010), workplace frauds (Albrecht & Albrecht, 2004), prisons as criminal classrooms (Kemp et al., 2019), consultancy services (Mohliver, 2018) and anonymous online hacker sites, in terms of malware (Hutchings & Holt, 2015). Essentially, learning via social networks involves knowledge transfer via interpersonal relationships (Nash, Bouchard, & Malm, 2013), whereas impersonal methods involve the spread of knowledge among criminals via a range of mediums including the media, archival sources,

[27] Nieto-Gomez (2016) applied the analysis of indirect coordination generally linked to the study of insects to the analysis of the indirect interaction between law enforcement and drug cartels.

online forums and government documents (Baker & Faulkner, 2003). Instances of diffusion via impersonal modes include the use of online forums where other users leave detailed instructions on hacking approaches (Zhang et al., 2015), virtual criminal apprenticeships (Hutchings & Holt, 2015), repeat domestic violence offenders having greater knowledge of the criminal justice system (Aguirre & Lane, 2019) and criminals researching potential sanctions (Goldstraw-White, 2011). However, Baker and Faulkner's (2003) two types of diffusion of fraud model cannot account for all forms of criminal learning; for instance in cases involving first-time offenders acting in isolation.

Two general fields of research—burglary and online hackers—have provided useful insight into the learning behaviours of criminals. Classifying some burglars as planners, Bennett and Wright (1984) suggested they scope residential addresses to ascertain whether occupants are home or enter the business during work hours to scope security features and identify valuable items. Generally, rule-of-thumb approaches that build on previous learning and experience are used by burglars to weigh up options (Taylor, 2013). However, more experienced burglars engage in detailed research—reading magazines on stately homes looking for antiques and then researching the value of specific items in libraries (Meenaghan, Nee, Van Gelder, Vernham, & Otte, 2020). In the related field of commercial robberies, experienced offenders are highly attuned to situational cues that indicate vulnerability demonstrating greater levels of métis than novice offenders (D'Alessio & Stolzenbery, 1990). The study of terrorist events provides further insights into crime métis: for instance, half of all al-Qaeda terrorist attacks occur within a 17-mile radius of the criminal's residential address, highlighting the role of métis in target selection (Smith, Roberts, & Damphousse, 2016). An example of proximal connections to locations of interest is the Boston Bombings: the Kyrgyztani–American brothers Tamerlan and Dzhokhar Tsarnaev lived locally and were familiar with their selected operational theatre.

Online hacker and dark web communities also display variation in learning behaviours that correlates with the criminal experience of forum members (Alazab & Broadhurst, 2016; Hutchings & Holt, 2015). In one study, *novice hackers* sought the greatest level of information and shared the least, while *learning hackers* asked more questions and at the same time shared more knowledge as their experience increased (Zhang et al., 2015). *Causal hackers* paid attention to the latest information on internet communications, and *guru hackers* provided the greatest level of information to other forum members and sought limited information themselves (Zhang et al., 2015). Online hacker forums in this sense are knowledge transfer sites that reveal how an individual's learning behaviour changes with experience. These sites also reveal the provision of paid-for tutorials where novice hackers learn specialist criminal skills from more experienced operators (Hutchings & Holt, 2015). Similarly, novice hackers in some instances advertise their services as apprentices to more experienced hackers (Hutchings & Holt, 2015, p. 602).

Finally, a recent example of research where learning was assumed is that by Maimon et al. (2020, p. 3), who focussed on the modus operandi of email fraudsters, and contended that 'fraudsters take advantage of heuristics in judgments and biases in decision making to create circumstances that increase the likelihood of poor decision-making by potential targets'. The acknowledgement of heuristic shortcuts in the problem-solving processes of email fraudsters supports the assertion that learning is an integral component of financial crimes and thus should be included in any procedural examination of fraud.

3.4 Planning and Preparation

While some crime types require limited preparation, others require effort. This section examines the literature on criminal planning. It aims to confirm the validity of *planning* as a temporal element in financial crimes. Planning is defined as '[a]n organised and especially detailed method according to which something is to be done' (Stevenson, 2007, p. 2230).

Planning includes any cognitive or physical activity that relates to who will do what, where, when and specifically how, to overcome controls. Preparation may involve designing artefacts such as requisition orders, false cheques and procurement orders in a way that helps them to be passed off as genuine. It also involves consideration of the way the crime will be implemented to reduce risks associated with detection, to cover up activities that may link evidence to suspects, or to arrange an alibi for participants in the crime.

3.4.1 Offender Planning

The planning of financial crime has received less academic attention than other crimes such as burglary and robbery, but insights can be drawn from these crimes. Gill (2000), who concentrated on the planning of commercial burglaries, found that few of the 341 incarcerated burglars planned their crimes, while the majority reacted to an opportunity (Felson & Boba, 2010). Reflecting on this, two caveats must be considered: first, the dataset is drawn from incarcerated burglars (Ditton, 2001); and second, a majority of their crimes were amateurish (Gill, 2000). However, those who planned did so to tackle more valuable targets (Gill, 2000), and thus increased planning was associated with increased reward.

A key aspect of criminal planning is the selection of targets. Target selection implies a level of agency; that something is selected, and someone is selecting (Jacobs, 2010). Target selection occurs naturally; for instance via daily routines and legitimate visits to businesses (Gill, 2000). However, it is also engineered through the subversion of insiders. Cornish (1994) suggested networks should not be interpreted solely as connections between criminals, but also as connections between offenders and their victims. This highlights the role of both opportunity and agency in target selection because this is likely to impact the planning that takes place from the point of identification until the commission of the crime. Therefore, despite suggestions that crime does not occur without opportunity, opportunity can nevertheless be engineered (Gill, 2000).

Extending target selection beyond opportunity, Bennett and Wright (1984) identified two types of burglar: the searcher and the planner. The searcher, after deciding to offend, seeks a target. In contrast, the planner takes time between the discovery of a potential target and the commission of the offence (Bennett & Wright, 1984). Planning in this sense is described as 'any forethought concerning the execution of the offence' (Bennett & Wright, 1984, p. 47). This description is broad enough to include offenders who simply consider the various options of when to commit the crime and how to get away with it, as well as those that plan in a more detailed manner. Some burglars in one study disclosed a tendency to locate a potential target and then go away and think about it for a while, or to sit and watch it for a few days; while others admitted greater levels of planning went into their crimes. Some, depending on access, would scope the outside of the address and when they could go inside—like those planning to rob businesses—they entered legitimately to scope the target, then left to commit their crime later (Komesar, 1973).

Planning is not a static phenomenon; instead, planning differs between the novice and the professional criminal (Cromwell, Olson, & Avary, 1991). Indeed, Sutherland (1947) alluded to varying levels of criminal capability when comparing a criminally mature 14-year-old pickpocket with a criminally immature 60-year-old first-time fraudster. Cromwell et al. (1991) found relatively little evidence of planning conducted by novice burglars. However, by the journeyman stage, planning had emerged, while the professional burglar displayed complex behaviours consistent with highly effective planning, technical skills and organisational abilities. These few experienced individuals, according to Cromwell et al. (1991), generally did not carry out opportunity crimes; instead, they deliberately planned their crimes.

Other variables affect the nature of criminal planning. Cromwell et al. (1991) suggested the criminal who identifies an opportunity generally tends to carry out little

planning; in one example the planning entailed simply checking whether there were occupants present immediately before the crime. Although Wheeler et al. (1988) highlighted the role of what Felson and Boba (2010) later called specialised access, the requirement for an opportunity to access financial systems through which specific crimes may be committed highlights that where criminal opportunity is blocked, planning is necessary.

3.4.2 Decision Making

Understanding decision making requires understanding rationality (Secchi, 2011). Building on the works of Simon (1959), Becker (1962, p. 1) contended that 'rational behaviour implies consistent maximisation of a well-ordered function, such as a utility or profit function'. The outcome of this was an economic framework suggesting decisions to offend are based on the idea that crime pays when gains exceed costs (Allen, 2011). de Jonge (2012) argued rationality has three separate characteristics: the capacity to identify and use the most appropriate resources; the ability to use scarce resources in the most efficient manner (Allen, 2011); and the allocation of resources to provide the greatest level of utility for the individual (Becker, 1968).

Decisions to offend, when viewed from a rational choice perspective, are complex ones. Placing rationality at the centre of their discussions, Allingham and Sandmo (1972) proposed the choice to offend—in this instance tax evasion—was complex as a failure to disclose taxable income does not automatically trigger a reaction from tax authorities. Rather, it triggers the possibility of a reaction. In this way, when the options are limited to 1) do not offend, or 2) offend, with no penalty, it can be assumed that the decision to offend results in a better net result for the criminal; and, where a reaction by the taxation authorities is triggered then the criminal is worse off than had they selected the lawful option in the first place (Allingham & Sandmo, 1972). Such decisions, according to Secchi (2011), imply choice and are different from decisions that are described as mechanical or automatic. Allingham and

Sandmo (1972) also demonstrated that criminals consider the likely administration of penalties by taxation authorities on the difference between actual income and declared income. This penalty, it is assumed, would be higher than the taxation that would have been assessed against the taxpayer had they properly disclosed their full income. In these situations, decision makers face variables such as not knowing what the likelihood of detection is, or the potential penalty (Allingham & Sandmo, 1972); therefore such decisions are reflective of probabilistic choices rather than mechanical decisions (Secchi, 2011).

Not all criminals deliberate so fully. Instead, without prior consideration, some simply make automatic decisions and commit a crime (Secchi, 2011). This might then be followed by choice-framed decisions on how the criminal should commit their crime; thus the seemingly decisive individual may also demonstrate more refined decision making. The difference between considered and mechanical decision making is the time allocated to weighing the pros and cons before a decision is made (Secchi, 2011).

Decisions based on a choice perspective imply the individual considers alternative paths to an identical outcome. Creativity in decision making produces alternative options on which to base future choices, thus linking back to the categorisation of choice decisions (Secchi, 2011). For the fraudster, more choices and better alternatives provide better results. This is important for the current research as it accounts for the complexity of the decisions that offenders make. For example, criminals weigh up the likelihood of detection and make decisions to shield themselves from detection; while decision activities do not always mitigate these risks, they nonetheless reduce the likelihood. Thus, where in the past statistical calculations were used to understand factors that influence decisions (Allingham & Sandmo, 1972), it is important to remember these decisions were influenced by the creativity and the awareness of offenders as to the likelihood of detection.

3.4.3 Limiting the Chance of Detection

The outward appearance of legitimacy, which translates to a hypothetical ‘how can I commit this crime while seen to be acting legitimately?’ is crucial. This includes working out how to commit the fraud, how to overcome guardianship and, importantly, how to remain undetected (Benson, 1985). Success in this sense is determined largely by decisions made by the criminal because the environment only provides concealment to those who can blend in (Ekblom & Tilley, 2000). Examples of efforts taken to lessen the likelihood of suspicion include two parties involved in price fixing arranging to meet at a trade fair, where it would not be unusual for them to be there at the same time, or minimising the number of telephone calls and not being seen together when travelling (Geis, 1970).

The avoidance of detection is a feature of fraud. Van Koppen and Jansen (1998, p. 232) contended that ‘to overcome security measures, [offenders] have to put more energy into preparations, have to plan more carefully, and divide up tasks’. Such efforts include shifting funds to cover holes in balance sheets at audit time (Riemer, 1941), as was the case in the Lehman Brothers matter, where Repo 105 transactions—the reclassification of loans as sales—were used for short periods. These transactions allowed Lehman Brothers to shift bad assets off their books, recording them as sales instead of debt and thus fraudulently covering up a deficit (Valukas, 2010). This provides for Vona’s (2008, p. 8) assertion that ‘there is a direct correlation between opportunity to commit fraud and the ability to conceal the fraud’.

3.4.4 Evolution of Offending

The intended outcome of deliberate efforts to limit detection results in an evolution of offending methodologies. As with the evolution of species, ecosystems and social environments over time, the evolution of fraud is an example of environmental changes through technological and administrative processes (Ghazi-Tehrani & Pontell, 2021; Schroeder, Pepper, & Nettle, 2014). As control mechanisms evolve, the professional fraudster

evolves in a ‘co-evolutionary arms race’ alongside control systems (Brown, 2017). As controllers introduce control mechanisms based on previous crimes, failure signals alert the fraudster to their detection and this drives further criminal adaption (Ghazi-Tehrani & Pontell, 2021). The cycle continues to repeat until one or the other ceases their adaptation (Nieto-Gomez, 2016). Evolution also occurs via the spread of methods transferred by individuals as they move from one criminal syndicate to another. Conceptualising this as a form of bacterial conjugation, Jones (2019) mapped the spread of innovative criminal tactics across Mexican drug cartels instigated by the movements of individuals between cartel organisations.

Ekblom and Tilley (2000) hypothesised a lack of criminal talent or innovation would result in nothing more than parry and thrust between the fraudster and those charged with preventing the fraud. However, if the fraudster is innovative observers are likely to see greater levels of evolution. This, it would seem, should certainly be the case with the ongoing evolution in fraud controls over recent years in response to seemingly increasing levels of fraud. The difficulty of controlling such illicit behaviours was aptly expressed by Lashmar and Hobbs (2018, p. 106) who contended that ‘organised crime draws upon skills emanating from a legitimate business and, that for legitimate businesses, illegal activities can sometimes become completely interwoven with their daily pattern of activities’, a point borne out by the maximiser adaptation to strain theory (Murphy & Robinson, 2008).

3.4.5 Collaboration

Another area linked to planning that has received attention is collaboration. While the fraud triangle is based on the premise of the individual fraudster (Cressey, 1953), not all frauds can be carried out by a single criminal; instead, knowledge and skills deficiencies often necessitate criminal collaboration (Weerman, 2003). For crimes where a single fraudster is involved, this is often because of sufficient levels of access, knowledge and skills,

which is reflected in lower-value crimes. However, most complex frauds necessitate collaboration in some guise, as was evidenced in the Bernard L. Madoff Ponzi Scheme, popularly referred to as an individual crime when in fact the scheme necessitated the involvement of up to 14 co-offenders (Hardy et al., 2020; Lewis, 2013a, 2013b). Indeed, Ekblom and Tilley (2000, p. 387) theorised that the complexities of crime 'entail bringing together a range of human and physical resources in a division of labour'; thus an absence of necessary skills must be overcome by the inclusion of a collaborator to fill skills shortages.

Collusion in frauds targeting organisational victims overrides a range of crime prevention measures including the separation of duties (SOD) and oversight (Dorminey et al., 2010; Weerman, 2003). Therefore, collaboration, and with it the bringing together of shared resources in the attainment of a crime, is an important consideration when seeking to understand how crimes occur (Ekblom & Tilley, 2000). Weerman (2003, pp. 399-401) identified several collusive characteristics: 1) offenders vary in their preference for co-offending or solo offending, 2) differences between offence types, 3) younger offenders collude more, 4) generally initiated by one of the co-offenders, 5) complexity of collusion varies from simple to complex interactions, 6) collusion is generally seen in smaller group settings, 7) homogeneous offending groups, and 8) co-offending groups remain in an almost constant state of flux with membership evolving and changing, often because of changing needs or drivers.[28]

These occurrences were condensed by Weerman (2003, pp. 401-403) into three perspectives: the 'group influence perspective' identifies collusion as the by-product of group pressure, similar to Sutherland's (1947) differential association theory; the 'social selection perspective' identifies collusion as an outcome of like-minded individuals seeking out others

[28] Weerman (2003) synthesised several co-offender studies to better explain how co-offending is established and implemented (Canter & Alison, 2000; McCarthy, Hagan, & Cohen, 1998; Reiss, 1986, 1991; Tremblay, 1993; Warr, 1996; Zimring, 1981).

with similar views, beliefs and or goals; and the ‘instrumental perspective’ identifies collusion as the result of offenders identifying the probability of collusion bringing success to a criminal endeavour. In a similar fashion, Free (2015, p. 187) suggested three archetypes of co-offenders as ‘individual-serving functional bonds’ where co-offenders determine that a joint enterprise would be more profitable; ‘organisation-serving functional bonds’ where collusion advances not the individual but the organisation; and ‘affective bonds’ characterised by deep levels of connection by either kinship or friendship.

3.4.6 Resources

An important study in the field of white-collar crime as it relates to how offenders commit their crimes was advanced by Ekblom and Tilley (2000), who proposed the importance of resources. From a purely rational choice perspective, decision making is linked not only to decisions to offend but also to the significance of the resources criminals bring to their crimes (Cornish & Clarke, 1986). Ekblom and Tilley (2000) and Cornish (1994) suggested that crimes require a series of acts over time, which suggests that criminals navigate a series of acts and decision points to prepare for and implement their crime. This points to the possibility that each stage of the offending process likely requires a different set of knowledge, skills and techniques. Ekblom and Tilley (2000) identified five resource categories. The first three—personal resources, cognitive resources and moral resources—arise from within the offender, while facilitatory resources and collaborative resources arise externally from the offender.

The learning criminal develops cognitive resources as they interact with a range of learning opportunities. Such resources include learning how a financial system reacts to a particular illicit incursion or the methodology of committing embezzlement. Learning also provides for the criminal insights into which targets are more suitable than others (Ekblom &

Tilley, 2000). This process of learning directly influences the choices made by offenders about how they implement their crimes.

Cressey (1953) and Morales et al. (2014) contended that the fraudster attempts to distance themselves from their criminality and normalise as much as possible their actions. The moral resources proposed by Ekblom and Tilley (2000) explain that offenders need to overcome moral scruples to rationalise or neutralise their behaviour (Sykes & Matza, 1957). Facilitatory resources are the physical instruments of crime and include the software necessary to overcome a computer system firewall, magnetic strip readers, and card coding machines necessary for the theft of credit card details and the associated spending. Finally, Ekblom and Tilley (2000, p. 383) proposed collaborative resources or 'an appropriate skill-mix and capacity' work together in the completion of the crime. In this case, the absence of a necessary skill set is addressed by the inclusion of a collaborator in possession of the skills, techniques or knowledge necessary to execute the crime. The resources an offender possesses have the potential to shape the nature of the crime; for instance, if they do not possess the skills necessary to defeat one fraud control, they may switch to an alternative system they do have the resources to overcome. It is also possible that in the case of complex fraud, an occupational position is a resource. From the perspective of cognitive resources an occupational position provides the individual with the necessary knowledge, skills and potentially techniques needed to commit the crime. An occupational position as a resource may also provide insider fraudsters with the facilitatory resources needed to commit a crime; for instance in the case of insiders assisting outsiders in a criminal endeavour.

3.5 Summary

The criminology literature historically focusses on questions of 'who' and 'why' (Braithwaite, 1985), with Levi (1984, p. 322) suggesting that '[i]n their obsession with the motivational issues surrounding why people do what they do, criminological theorists have

tended to neglect the equally (if not more) important issue of how they are able to do what they do'. Indeed Edelhertz (1970, p. 4) asserted that 'the character of white-collar crime must be found in its modus-operandi and its objectives rather [than] in the nature of the offenders' (Smith et al., 2011).

Studies addressing specific crimes including anti-trust violations (Geis, 1970), computer crimes (Grabosky & Walkley, 2007), consumer fraud (Rothschild & Thorne, 1976), corporate crime (Ghazi-Tehrani & Pontell, 2015), embezzlement (Cressey, 1953; Riemer, 1941), guanxi—institutional bribery (Pontell, Ghazi-Tehrani, & Chang, 2017)¸ long firm frauds (Levi, 2008) and tax evasion (Allingham & Sandmo, 1972), have provided rich descriptions, setting the standard for those seeking to explain how frauds are committed. Other studies have addressed a range of separate behavioural and procedural aspects that begin to unpack how frauds occur, including insider threats (Australian Government, 2016), rationality (Becker, 1962, 1968), planning behaviours of burglars (Bennett & Wright, 1984), criminal learning (Allan, 2018), rationalisation (Benson, 1985; Cornish & Clarke, 1986; Sykes & Matza, 1957), criminal resources (Ekblom & Tilley, 2000) and the prevalence of so called copycat frauds (Pontell & Geis, 2014).

The opportunity presented by these disparate studies for those who seek to fill the gap identified by Edelhertz (1970), Levi (1984), Braithwaite (1985) and Free (2015) is twofold. The first opportunity is to address the absence of a consistent framework of analysis against which to understand crimes. The adoption by Geis (1970), Cressey (1950) Bennett and Wright (1984), Levi (2008) and Riemer (1941) of a highly descriptive, often case-driven approach that often involved post-crime offender interviews, prison and courtroom observations stands in contrast with the secondary data-driven theoretical explanations of behaviour by Allingham and Sandmo (1972) Rothschild and Thorne (1976) and Becker (1962, 1968). The strength of case-driven research is its capacity for researchers to provide

detailed explanations of the ‘social processes that unfold between persons participating in the [crime]’ (Swanborn, 2010, p. 13). The second opportunity relates to the absence of studies bringing together a diverse array of crimes with the express intention of drawing comparisons between how different frauds are executed.

The introduction of the ALPi Model allows a thematic appraisal and helps to negate the potential drawback of tightly focussed case study research by facilitating examination of a wider variety of frauds in the one study, while also benefiting from a case study’s ability to provide a rich and detailed account of phenomena under observation. While the validity of the framework of access, learning and planning—as evidenced in the review of empirical studies—was supported, the data presented were limited to addressing the interests of other studies. Therefore the capacity of the ALPi Model’s three temporal elements to comprehensively outline how frauds are committed could not be fully gauged using previous studies. However, it is suggested that collection of data to specifically test the validity of the ALPi Model for producing new insights into how frauds are committed is necessary, rather than relying on previous research. The next chapter outlines the methods adopted in this thesis.

Chapter 4: Methodology

This thesis seeks to identify differences in temporal and behavioural patterns between fraudsters classified as either insiders or outsiders. The units of analysis in this thesis are frauds investigated by units of the AFP and the NSWPF. The selection of individual crimes as the 'units of analysis' directly influenced the research design, as data may be drawn from criminal case management files and interviews with detectives, as well as from an examination of court-produced pre-sentencing reports, which suggests a thematic approach to the analysis of data (Axinn & Pearce, 2006, p. 29). The selection of a methodological framework generally guides the identification of appropriate methods for data collection (Hesse-Biber, 2010, p. 455). Financial systems are often viewed via a quantitative, dollars and cents frame. However, it is how the offender operates within that financial environment, how they learn, respond to barriers and controls and what they view as strengths and weaknesses that dictates the adoption of a qualitative mixed-methods framework through which to guide this thesis (Hesse-Biber, 2010, p. 456; Morse & Richards, 2002; Watkins & Gioia, 2015). Patton (2002, p. 4) suggested the use of direct observation, interviews and document analysis when following a qualitative mixed-methods methodological framework. However, because of the nature of the illicit activity of frauds, direct observation was neither possible nor desirable. Consequently, this thesis was based on a number of cases, as these are more likely to provide data to answer research questions focussing on 'how' (Yin, 2014). Each 'case' consisted of participant interviews and police case management files that contained audio files in the form of electronic records of detectives' interviews with offenders as well as research interviews with participating detectives; thus audio file analysis was also used to provide data.

A qualitative mixed-methods methodological framework allowed the researcher to understand the forces shaping the processes that individual fraudsters go through as they plan,

prepare for and carry out their crimes (Hesse-Biber, 2010, p. 456). This approach enabled the investigator to explore fraudsters' response to the unique settings they operate within, thus allowing a deeper, richer and more complete understanding of fraudsters' access, learning and planning behaviours (Morse & Richards, 2002; Watkins & Gioia, 2015).

A non-probability, purposive sampling approach was adopted to identify detectives and units of analysis to aid the researcher in understanding the phenomenon (Gill, 2020). This allowed the researcher to identify suitably experienced individuals with demonstrated expertise in the investigation of complex financial crimes (see Appendix A).[29] Another advantage was that it provided the researcher with the opportunity to elicit data from detectives to both address the stated research question, and aid in refining the framework of analysis that guides this thesis, specifically the ALPi Model outlined in preceding chapters.

To achieve the stated aims of this thesis, major themes were developed through a thematic analysis of the qualitative interviews and secondary data. Thematic analysis offers an efficient methodology to unpack subtle differences in the selection and implementation of tradecraft across complex fraud settings where differing levels of access have an impact on the manifestation of crime (Braun & Clarke, 2006; Kawasaki, 2019; Soltani, 2014). Thematic analysis is highly relevant as the themes in this thesis were subjected to a constant comparative approach that allowed for the identification of differences between the actions of insider and outsider fraudsters (Archer & Gartner, 1984; Boeije, 2002; Braun & Clarke, 2006). Thematic analysis also allowed for the identification of causal factors that drove differences between these crimes, and has been a popular choice for criminologists examining white-collar crime in the past (Grabosky, Braithwaite, & Wilson, 1987; Grabosky & Sutton, 1989; Kawasaki, 2019; Levi, 1993, 2010a). It is, however, not without its

[29] This method is sometimes referred to as 'expert sampling' where participants are selected primarily because they are best placed to provide reliable and valuable insights into the problem behind the research (Trochim, 2021).

criticisms. For instance, its inherent flexibility suggests the possibility of unconnected or incoherent themes emerging (Braun & Clarke, 2006; Holloway & Todres, 2003); there is a potential risk of 'cherry picking' themes or facts; and its flexibility has the potential to create uncertainty for novice researchers (Nowell, Norris, White, & Moules, 2017).

Finally, it is necessary to acknowledge the positionality of the researcher (Holmes, 2020). The catalyst for this study was the researchers professional background in law enforcement, specialising in financial crime investigation. Consequently, this thesis is shaped by a constructivist worldview (Creswell & Clark, 2007), one that identifies the experiences of individuals including criminals, victims, police officials and researchers as responsible for shaping perceptions of what truth is within the setting within which those individuals operate. Thus, from an ontological perspective, a relativist approach is adopted to understand what truth is (Holmes, 2020). From an epistemological perspective, an emic viewpoint shaped the design of this study and how it was conducted, as knowledge is shaped via interaction with the environment and those within it (Holmes, 2020). Therefore, the nature of the research problem posed within this thesis, the researcher's worldview and the nature of previous projects examining similar topics in areas other than fraud, strongly points to the adoption of a qualitative focussed methodological framework. In undertaking this study, the researcher acknowledged the presence of their worldview and the impact of their presence and role on the research as they sought to uncover and develop knowledge in conjunction with research participants.

4.1 Ethical Approvals

The Australian National University (ANU) requires all persons researching at ANU to undertake that research in compliance with the *Responsible Conduct of Research* policy (Australian National University, 2021). The ANU Human Ethics Committee approved two

protocols in relation to this research, on 7 November 2014 and 5 December 2014.[30] [31] The approved protocols were then sent to the relevant law enforcement agencies, along with the participant selection criteria (see Appendix A) and the Participant Information Sheet (see Appendix B). Both the AFP and the NSWPF subjected the protocols, selection criteria and participant information sheets to their own in-house ethics approvals processes. On 29 July 2015, formal approval was received from the AFP to interview participants and collect criminal prosecution files.[32] On 27 August 2015, formal approval was received from the NSWPF to interview participants and collect criminal prosecution files.[33] At this point, Participant Information Sheets (see Appendix B), and Written Consent Froms (see Appendix C) were distributed by liaison officers to detectives in the relevant squads, along with an invitation to participate in the interview (see Appendix D).

4.2 Qualitative Interviews

Semi-structured qualitative interviews are guided conversations with participants that are useful for understanding the intricacies of an event, as they provide participants with the opportunity to share information, meaning and opinions (Brennen, 2017, p. 29). Face-to-face, semi-structured interviews are appropriate with professional participants like police officers as they assist in unpacking complex issues (Gillham, 2005; Kleck, Tark, & Bellows, 2006).

4.2.1 Semi-structured Interview Process

The AFP provided the researcher with the contact details for detectives who had indicated a willingness to take part in the interviews. These interviews were arranged around the work commitments of the detectives and were conducted in person and, where operational

[30] Protocol 2014/564: provided ethics approval to conduct semi-structured interviews with detectives from two Australian law enforcement agencies.
[31] Protocol 2014/728: approved the collection of criminal prosecution files held by two Australian law enforcement agencies.
[32] Case 12 / Case 13
[33] Case 01 / Case 02 / Case 03 / Case 04 / Case 05 / Case 06 / Case 07 / Case 11

requirements dictated, over the phone.[34] The NSWPF invited the researcher to NSW Police Headquarters, supplied a room and asked suitably experienced detectives to meet with the researcher.

Detectives that met the criteria were again supplied with a Participant Information Sheet immediately before the interview (see Appendix B). On the day of the interview, participants signed the informed consent form (see Appendix C). Detectives who agreed to be participants were advised they were able to withdraw at any time without repercussion (see Appendix B). Participants were not offered inducements to take part in the interview and while the interviews were to be audio-record, participants were advised they could decline to be audio-recorded. All participants agreed to have their interviews audio-recorded, and there were no foreseeable risks to the participants from taking part in the interviews.

Interview participants were drawn from specialist fraud investigation units within the two police forces. Investigators were selected on their ability to demonstrate a minimum level of experience (see Appendix A). Participants were later asked to identify relevant criminal cases that met a set criterion (see Appendix F). These would later become the main units of analysis.

Participants were then asked a series of questions (see Appendix E). These questions focussed on three general areas:

1. the relative expertise of the participants and how that aided their investigation of complex frauds.
2. their observations about fraud cases in general with which they had dealt throughout their careers
3. observations of one specific case that would later become a unit of analysis.

[34] Case 13 – as the participant was based interstate it was agreed a telephone interview would be appropriate.

Interviews were scheduled to last 60–90 minutes. While all participants agreed to have their interviews recorded and transcribed, they occasionally provided information they later advised had to be 'off the record'. Off-the-record discussions were omitted from the analysis and are not included in this thesis. Because of the collaborative nature of criminal investigations, some interviews were conducted with two participants. In these instances, their responses were recorded, transcribed and analysed both separately and in conjunction with each other, given the tendency of some participants to talk over each other. Only one participant was interviewed twice, because they introduced a second case that became a further unit of analysis.

4.2.2 Data Collection

Eighteen detectives were interviewed, 3 from the AFP and 15 from the NSWPF. One AFP participant recommended a single criminal case as a unit of analysis, while the remaining two participants each offered two criminal cases as units of analysis. Of the 15 NSWPF participants, 13 offered one criminal case as a unit of analysis, and the remaining two participants each offered two criminal cases as units of analysis. The detectives had an average of 19.2 years of police experience each.

While the interviews were scheduled to last between 60 and 90 minutes, the average time was 180 minutes, with some continuing to 240 minutes. The interviews were structured to ease participants into the process using initial questions based on areas familiar to them. As the interviews progressed the questions became more specific, thus requiring increased effort on the part of the participants (Gillham, 2005). As evidenced by the average length of time taken, the participants were positively engaged with the process. The interviews came to a natural conclusion at the point of data saturation, which, according to Bowen (2008, p. 140) is when 'the researcher gathers data to the point of diminishing returns'. Interview notes were made by the researcher and augmented by an electronically recorded record of the interview.

A transcript of the interview was then professionally transcribed and checked by the researcher, and all quotations used in the thesis were checked and re-transcribed by the author (Chang, 2010).

4.3 Secondary Data

During the qualitative interviews, each participant described a case they had investigated in the role of officer in charge (OIC). The OIC role in a criminal investigation is generally held by a detective with experience in complex investigations. In total, 22 cases were put forward by the participants; 5 from the AFP and 18 from the NSWPF.

4.3.1 Data Collection

As already described, the interviews were split into three stages, with stage three questions referring to the fraud case management files proposed by the participants (see Appendix E). In addition to the questions asked in stage three of the interviews, participants provided electronic copies of the case management files. These electronic copies were secured by the researcher and subjected to further analysis.

As outlined in Table 3, specific coding references were applied to link related cases and individuals. For example, all case management files collected from the AFP and the NSWPF were given an initial numerical code commencing with ‘01’. The participants that were interviewed were given a numerical designation linked to the case; so in this instance, the study participant was coded as N01, additionally lower case letters were added to denote more than one participant being interviewed, e.g.’ N01a, N01b. While the principal fraudster was PF01 and associate fraudster was AF01. Witnesses and victims in this particular case were coded OT01.

Table 3

Data Coding

Case (case management file)	**Case 01, 02…**
Participant (detective)	N01, 02…
Principal fraudster	PF01, 02…
Associate fraudster	AF01a, 01b, 02a, 02b…
Other (witness/victim)	OT01a, 1b, 02a, 02b…

The contents of the electronic cases management files varied in their makeup. Typically, a case management file is a collection of both documentary and electronic materials collated by police during a criminal investigation. This will include, at a minimum, statements from victims, witnesses and police officers, along with documentary evidence alleged by the police to support the charges against the accused. This includes facts sheets—documents compiled by prosecuting authorities that set out the charges and evidence against an accused before the initial hearing (Western Australia Police Service, 2016). In total, 872 separate documents, including the interview transcripts, were collated by the researcher (see Table 4).

Table 4

Secondary Document Types

Document type	Number
Participant interview transcripts	22
Facts sheets	69
Accused interview transcripts	14
Victim and witness statements including police statements	220
Post-operational assessments	3
Bail submissions	13
Briefs of evidence	1
Telephone intercept files	319
Telephone intercept transcripts	2
Listening device transcripts	42
Surveillance transcripts	6
Court transcripts	23
Psychological reports	1
Judges sentencing reports	1
Assorted other evidential documents	131
Media reports	5
Total	872

4.3.2 Data Assessment

The types of crime recorded across the 23 cases varied, with 15 unique frauds identified. Of the 23 cases, 10 were excluded (see Table 5). Three tax evasion cases,[35] one finance application fraud,[36] two identity frauds,[37] one account takeover fraud,[38] and one money laundering case were discounted because of a lack of case data sufficient to validate the participant interview transcripts.[39] Two further cases were rejected because they did not meet the case selection criteria—the first[40] because it focussed on

[35] Case 20 / Case 21 / Case 22
[36] Case 16
[37] Case 17 / Case 18
[38] Case 19
[39] Case 14
[40] Case 23

the illegal manufacturing of identity bundles (see Appendix F);[41] and the second because it was a romance fraud.[42] This left 13 case management files that were examined as units of analysis in this thesis (see Table 6).

Table 5

Excluded Case Descriptions

Case management files	Law enforcement offence description
Case 14	Money laundering
Case 15	Relationship fraud
Case 16	Finance fraud
Case 17	Identity fraud
Case 18	Identity fraud
Case 19	Account takeover fraud
Case 20	Tax evasion
Case 21	Tax evasion
Case 22	Tax evasion
Case 23	Manufacturing false identification documents

[41] An identity bundle refers to a collection of stolen or forged identify documents that, when brought together, help to satisfy 100-point identity checks applied by financial services institutions which consider credit applications submitted by potential customers. 'What we think was the Medicare card was generally used to support the driver's licences or bank card, so the 100 points, from what we can gather there was no fraudulent activity, no one has tried to claim a Medicare benefit, it's just to support the driver's licence' (Case 23 Participant Transcript).

[42] Case 15

Table 6

Selected Case Descriptions

Case management files	Offence description	Classification	Detective identifier
Case 01	Procurement fraud	Outsider	Detective N01
Case 02	Account takeover fraud	Outsider	Detective N02
Case 03	Mortgage fraud	Outsider	Detective N03
Case 04	Theft as an employee	Insider	Detective N04
Case 05	Credit/debit card fraud	Outsider	Detective N05
Case 06	Credit/debit card fraud	Outsider	Detective N06
Case 07	Debt-factoring fraud	Outsider	Detective N07
Case 08	Procurement fraud	Insider	Detective N08
Case 09	Theft as an employee	Insider	Detective N09
Case 10	Accountancy fraud	Insider	Detective N10
Case 11	Mortgage fraud	Outsider	Detective N11
Case 12	Superannuation fraud	Outsider	Detective N12
Case 13	Insider trading	Insider	Detective N13

4.3.3 Data Management and Analysis

The nature of the research problem, the available sources of data and the methodological framework point towards the adoption of an inductive-based analysis (Patton, 2002, p. 453). Given the nature of the data collected to this point, including paper documentation and transcriptions of audio interviews with detectives, NVivo software was used to assist in the thematic coding and analysis of patterns within the data. All data collected were subsequently separated into ‘units of analysis’ (Watkins & Gioia, 2015, p. 73). Contained within each unit of analysis were the transcripts of interviews with fraudsters and detectives, official court transcripts, police statements, witness statements, victim statements, facts sheets, intercept transcripts and other associated documentation that made up the case management files. The sample dataset included a total of 827 documents.

The transcribed detective interview transcripts were thematically analysed. Thematic analysis is the process of identifying and analysing patterns that exist in datasets (Braun & Clarke, 2006, p. 80). In identifying key salient points within the data, thematic analysis assisted in illustrating the presence of situational factors that influenced fraudsters' decision making, and this helped to reveal how fraudsters fit their approach to their crimes (Joffe, 2011, p. 209). The literature was engaged with early to assist in developing sensitivity to the more subtle features likely to be present in the data (Braun & Clarke, 2006, p. 88; Strauss & Corbin, 1998, p. 49); from an inductive perspective, this can also 'narrow your analytic field of vision' (Braun & Clarke, 2006, p. 86),

In preparing for the thematic analysis of the interview transcripts, they were reviewed for transcription errors (which were corrected) and duplications, and at the same time formatted for analysis (Watkins & Gioia, 2015, p. 73). This process of re-listening to the recorded interviews and reading the transcripts allowed for familiarisation with the data, and initial notes were made of potential coding frames that would be developed later (Braun & Clarke, 2006, p. 87). Initial codes were then developed when reading back through all data, and using the initial notes made from the first full reading of the data (Braun & Clarke, 2006, p. 88). Having earlier indicated the use of literature to inform the search for subtle patterns within the data, Braun and Clarke (2006, p. 88) suggested theory-driven coding commences with broad questions around which coding may be built. Such an approach, however, must not obfuscate emergent themes not previously considered. The next stage of analysis involved a search for themes in the earlier collated codes; here the intention was to look for codes that could be combined into meta themes (Braun & Clarke, 2006, p. 89). It is important to note that this was not a strictly staged process; rather it developed iteratively as the research moved back and forth between stages as new insights were gained and coded (Braun & Clarke, 2006, pp. 87-89). The fourth stage of the analysis began with a review of the

themes identified in the previous stage. From there they were refined to develop a coherent narrative in both the individual themes and the dataset as a whole (Braun & Clarke, 2006, p. 91). The final stage involved defining and naming the themes to establish what was important and critical about each (Braun & Clarke, 2006, p. 92). By way of an example, a theme that emerged during the planning stage of the case narratives was later referred to as 'backstopping'. Backstopping, as explained further in Chapter 8, is a process adopted by fraudsters to provide a veil of legitimacy to a fraudulent material fact.

Following the thematic analysis, the units of analysis were separated based on proximity to the financial system as a key variable. In this case, 'proximity to financial systems' was determined by whether a principal fraudster was an insider in the victim organisation or an outsider. This resulted in the identification of five insider cases and eight outsider cases. Having separated the two datasets, a comparative analysis process was adopted to identify the presence of variation between them. The analysis identified several differences, ranging from subtle to significant, between how fraudsters as insiders or outsiders gained access, acquired the necessary knowledge and information, and finally planned their crimes.

4.4 Summary

Drawing on the nature of the problem, the shape of the research question and the potential sources of data available to the researcher, this chapter has described the methodological framework underpinning this thesis and the methods adopted to address the research question. Combining interviews with detectives, case management files and other secondary information sources into distinct units of analysis provided a comprehensive overview of the activities of fraudsters throughout their fraud event timeline. A thematic approach was adopted given the diversity of data that were primarily represented in a textual

format (Braun & Clarke, 2006). The next chapter provides a synopsis of each of the 13 cases on which the subsequent analysis was based.

Chapter 5: Results

Interviews with detectives were combined with 13 case management files drawn from the AFP and the NSWPF to produce 13 case synopses.[43] Each synopsis was compiled to provide a concise overview of the relevant criminal case. Therefore, each synopsis was given a unique case identifier, each research participant was given a unique identifier and each offence committed by the fraudster or syndicate was linked to the cases. In addition to this and without disclosing identities, each fraudster was given a unique identifier and their role in the fraud was briefly described. Relevant victims, witnesses and other associates were also identified using unique identifiers that did not disclose their natural identity.

5.1 Case 01

Case identifier	**Case 01: Financial institution procurement fraud**		
Participant identifier	N01		
Source	New South Wales Police Force		
Offence	1x249B Crimes Act 1900 (NSW) Corrupt commissions or rewards 1x192E Crimes Act 1900 Fraud		
Offender identifier	Identifier	Classification	Role
	PF01a	Principal fraudster	Chief executive officer (CEO) of an offshore information technologies (IT) company
	AF01a	Associate fraudster	Executive general manager of infrastructure and operations at the victim organisation
	AF01b	Associate fraudster	General manager of engineering at the victim organisation

[43] Financial crime-related offences in the Australian Federal Police jurisdiction fall under the Corporations Act 2001 and the Criminal Code Act 1995. New South Wales financial crimes offences fall under the Crimes Act 1900.

Case identifier	Case 01: Financial institution procurement fraud		
	OT01a	Witness	Whistle blower
	OT01b	Other	Director of a shelf company at the bequest of PF01
	OT01c	Other	Victim organisation contractor and equity holder in PF01's company, who introduced PF01 to AF01a and AF01b
	OT01d	Other	Employee of company owned by PF01

Case 01 was a criminal investigation into a fraud committed against a major Australian bank. Corrupt payments offered by PF01, the CEO of an international IT company, were made to two senior employees (AF01a & AF01b) of the victim organisation in exchange for preferential treatment in IT procurement. Between 2008 and early 2015, OT01c, an equity holder in the IT company, also worked as an IT contractor for the victim organisation where he introduced PF01 to AF01a and AF01b. In his IT contracting role, OT01c discretely provided insider information to PF01. Email records secured by police identified communications between OT01c, OT01d and PF01 where they discussed information that the victim organisation might stop buying IT from PF01's company. PF01 responded by saying 'if we are talking about outsourcing the entire existing [victim organisation] operations to [a competitor organisation] then [AF01a] will squash it', 'he [AF01a] isn't moving to Australia to do that, quite the opposite'.[44] An early example of the compromised nature of AF01a and AF01b was when AF01b unethically outsourced the development of an internal competitive positioning statement to OT01d—an employee of PF01—to ensure the positioning statement, when read by others in the victim organisation, would reflect favourably on the business of PF01. Consequently, PF01 won more procurement contracts.

In late 2013, PF01 was in negotiations with an international software conglomerate that sought to buy his IT company for US$260 million. The deal included a base payment; however, to trigger an additional performance-related pay-out, PF01 needed to demonstrate sustained

[44] Detective N01 suggested AF01a was, prior to his employment with the victim organisation, already loyal to PF01.

industry sales. Effectively, for every dollar over US$20 million earned between 1 January 2013 and 1 January 2014 PF01 would receive an additional US$10.15. However, nearing the end of the 12-month period, he had not reached the US$20 million target. To achieve this, PF01 convinced AF01a and AF01b to purchase overpriced and unnecessary IT software on behalf of the victim organisation. Where this occurred, PF01 stood to earn an additional US$135 million.

AF01a and AF01b worked on the unnecessary procurement deal worth AU$14 million. To facilitate this, they suggested PF01 become an accredited McAfee seller. The victim organisation had previously rejected a direct approach from McAfee, primarily because the victim organisation was already receiving this software as part of a bundle from a competitor of PF01. Despite knowing this, AF01b provided PF01 with the McAfee pitch documents and advised what to alter. PF01 altered the pitch and sent it back to the victim organisation where AF01a and AF01b signed off on the AU$14 million dollar purchase of the unnecessary software.

As the senior of the two associates, AF01a had financial delegation authority for AU$1 million. To facilitate the AU$14 million dollar purchase, AF01a and AF01b fraudulently structured the deal into 14 separate transaction documents to prevent internal oversight. However, OT01a, an internal whistle blower, questioned the validity of the purchase, unwittingly bringing it to the attention of his line manager, AF01b. Over the following 9 days, and despite ongoing protests from OT01a, the deal was approved by the victim organisation.

Within days of the sale, AF01a arranged for a restructure of the area in which OT01a worked. Despite a history of positive workplace assessments and positive feedback from other managers, OT01a had his employment terminated by AF01a. Following this, an intercepted email between AF01a and PF01 contained the following reference ’don’t worry, he’s gone, we restructured, and he was sacked’.[45]

Case 01 Discovery

This scheme was detected by internal audit functions that examined the questionable nature of the deal following the sacking of the original whistle blower.

[45] Detective N01 Transcript

5.2 Case 02

Case identifier	Case 02: Phone porting—account takeover fraud		
Participant identifier	N02		
Sources	New South Wales Police Force		
Offence	49x192E *Crimes Act 1900* Accessory before the fact to fraud 46x192J *Crimes Act 1900* Deal with identity information to commit indictable offence 35x192E *Crimes Act 1900* Accessory before the fact to attempted fraud 19x192E Crimes Act 1900 Fraud 15x308C *Crimes Act 1900* Unauthorised access, modification, or impairment with intent to commit serious indictable offence 11x192E(1)(a) *Crimes Act 1900* Dishonestly obtain property by deception 10x192E *Crimes Act 1900* Attempted fraud 10x192K *Crimes Act 1900* Possession of identification information with intent to commit indictable offence 7x93T *Crimes Act 1900* Participate in criminal group 2x193B *Crimes Act 1900* Knowingly deal with proceeds of crime intent to conceal 1x351A *Crimes Act 1900* Recruit person to engage in criminal activity 1x93T(1A) *Crimes Act 1900* Directing activities of a criminal group 1x193D *Crimes Act 1900* Deal with property intend to be an instrument of crime 1x256 *Crimes Act 1900* Make, possess equipment to make false document etc		
Offender identifier	Identifier	Classification	Role
	PF02a	Principal fraudster	Planning, setting up drop accounts deploying malicious software
	PF02b	Principal fraudster	
	PF02c	Principal fraudster	
	AF02a	Associate fraudster	Mules who withdrew stolen funds from accounts[46]
	AF02b	Associate fraudster	
	AF02c	Associate fraudster	
	AF02d	Associate fraudster	
	AF02e	Associate fraudster	

[46] See Broadhurst, Grabosky, Alazab, and Chon (2014) and Chabinsky (2010) for descriptions of mules in criminal syndicates.

Case identifier	Case 02: Phone porting—account takeover fraud		
	AF02f	Associate fraudster	
	AF02g	Associate fraudster	
	AF02h	Associate fraudster	
	AF02i	Associate fraudster	
	AF02j	Associate fraudster	
	AF02k	Associate fraudster	
	AF02l	Associate fraudster	Possessed stolen identities

Case 02 was a criminal investigation into an organised crime syndicate committing account takeover frauds. Three principal fraudsters, in this case, worked collaboratively to steal the identities of victims before taking control of their bank accounts. They also directed the activities of mules who, using the compromised identities, withdrew funds from victim accounts. In total, 39 mules were linked to this syndicate, 22 of whom operated outside New South Wales (NSW).

Initiation events, where fraudsters stole part or all of a victim's identity profile,[47] marked the beginning of each fraud. In one instance, PF02a and PF02b purchased stolen personal information from dark web portals known as carding sites.[48] Other instances involved hacking the computers of a financial planner and payroll companies. With these initial identity bundles, the fraudsters undertook what police described as a form of social engineering. For example:

they called up people, so if they are short on identification, they'd call up organisations, pretend they are [the victim] and tried to elicit some information they are short on, sometimes even the victim themselves. They pretended they are from [a] telco, and say I just need your confirmation of your account number if they are missing that, and they came up with some grand story that makes them sound legitimate.[49]

The fraudsters purchased forged drivers' licences and Medicare cards from fraudulent identity manufacturing syndicates, blending the victim's details with the photographs of mules. They scoured public websites such as land registries, credit check agencies and the Australian Securities and Investments Commission, all of which for a fee allow the public to check the

[47] In the context of these crimes an identity profile relates to personal identifiable information and might include a victim's name and date of birth, or their name and credit card number.
[48] A carding site is generally a dark web site where criminals sell stolen credit card data. Detectives in Case 02 also determined the criminal methodologies adopted by this syndicate were learned in these dark web carding sites where tuition was available for a fee.
[49] Case 02 Detective N02 Transcript

particulars of an individual. This provided additional information including tax file numbers, signatures, dates of birth, company names and addresses. They stole mail and cold-called clubs with which the victim might have an association to source additional information.[50] They also ported victims' mobile numbers, transferring them to other telecommunications providers, which gave them control over the victim's mobile phone apps including online bank accounts, email and MyGov data.

Blending stolen identities and forged identity documents, the fraudsters satisfied identification verification controls at banks where they opened new accounts and interacted with existing accounts (Allan, 2016). In one instance the syndicate gained control over a victim's bank account and transferred AU$200,000 to accounts over which they had control. In other instances, mules, using cloned credit cards, engaged in high-volume purchasing of high-value goods and setting up pre-paid credit cards that could be used later. They also committed several high-value eBay scams and cheque frauds, which suggested this was a diverse and agile syndicate, capable of targeting a range of vulnerabilities across numerous financial systems.

Case 02 Discovery

Unlike other crimes examined during this study, this case had multiple frauds underway against multiple individuals and organisations. This meant that detection was sporadic: in some instances banking institutions identified fraudulent transactions; in others, it was an online marketplace that detected an anomaly; and in others, it was the victim who had their identity stolen.

5.3 Case 03

Case identifier	Case 03: Mortgage and finance fraud
Participant identifier	N03
Sources	New South Wales Police Force
Offence	1x178ba(1) *Crimes Act 1900* Obtain money by deception 1x300(2) *Crimes Act 1900* Use false instrument with intent 1x319 *Crimes Act 1900* Do act etc with intent to pervert course of justice

[50] In one instance a fraudster called a golf club pretending to be the victim who was a member. In doing so, they asked what residential address the club had against their name, as they had recently moved address and wanted to ensure they were up to date.

Case identifier	Case 03: Mortgage and finance fraud		
	7x254(B)(Ii) *Crime Act 1900* Use false document to obtain financial advantage 1x315(1)(B) *Crimes Act 1900* Hinder discovery evidence re: indictable offence 1x327(1) *Crimes Act 1900* Make false statement on oath amounting to perjury		
Principal fraudster identifier	Identifier	Classification	Role
	PF03a	Principal fraudster	Acted as the public face of the syndicate organising finance deals
	PF03b	Principal fraudster	Organised crime boss with connections to Sydney underworld
	AF03a	Associate Fraudster	Acted as an office manager backstopping most of the frauds
	AF03b	Associate Fraudster	Unknown associate with experience in the construction industry
	AF03c	Associate Fraudster	Unknown role in one vehicle finance fraud
	OT03a	Victim	Identity stolen and used by the syndicate
	OT03b	Victim	Sales representative who worked for the heavy machinery victim organisation
	OT03c	Witness	Sales representative who worked for virtual office provider
	OT03d	Other	A local barrister who provided services for PF03a

Case 03 was an investigation into an organised crime syndicate committing mortgage and loan frauds. The syndicate was led by a self-styled finance broker (PF03a) and a Sydney crime

figure known to the police (PF03b). They 'set up deals and put people together to finance short- and long-term loans using fraudulent documents, using systematic methodologies to deceive financial institutions'.[51] PF03a and PF03b were supported by AF03a who worked behind the scenes to legitimise the fraudulent loans. Occasionally, other criminal associates joined the syndicate to support specific frauds.

On one occasion, PF03a convinced a victim, OT03a, to become the director of a new company, hereafter known as Company C03a.[52] In reality, OT03a was a director in name only. Using forged documents, PF03a applied for an AU$539,500 business loan against Company C03a, without OT03a's knowledge. PF03a diverted the funds into accounts over which he had control. He never made repayments. A civil action was then taken out against Company C03a and OT03a as the director. PF03a continued to make further loan applications, one for AU$125,000, an AU$179,835 loan for three vehicles, an AU$325,000 loan for a boat, an AU$63,000 loan for a further vehicle and an AU$140,000 loan for three motorcycles, each time relying on fraudulent business and tax return documents linked to Company C03a. Using another fictitious company, hereafter known as Company C03b, PF03a also sought an AU$1,200,000 mortgage for a Botany Road property in Sydney, and an AU$63,000 loan for another vehicle. The intention in each case was to make a fraudulent financial gain by deliberately failing to make repayments on the loans.

The syndicate also targeted a significant federally funded national infrastructure contract. Using fraudulent documents, they sought to acquire four heavy plant excavators, valued at AU$940,000. They arranged to lease the excavators to a legitimate construction company that had been awarded a federally funded infrastructure contract. The following discussion was captured using a legally acquired telephone intercept:

> PF03b: Are you interested in an excavator as well, it's got a 5-year contract and you make three grand a week out of it…
>
> PF03a: Yeah, if they do, I'll give you a history when I see you but if they get something, we will do whatever.
>
> PF03b: Oh, they will, it's like a permanent income, and this contract is real, it's with um, it's federally funded. It's all in writing, it's my mate who has been doing excavation

[51] Case 03 Facts Sheet
[52] Like the participants, the details of implicated business have been anonymised.

for 20 years, he's got the contract and he needs 60 of them, 25 tonners, so if we get one or two, it's a wage for us mate, it really is.

PF03a: Yeah, but have you got somebody who can set it?

PF03b: I've got [name of vendor finance company] who will do vendor finance.

PF03a: Oh beautiful, we'll just go and sign up today.

PF03b: I've got the invoices; [name of vendor finance company] will do vendor finance. You know we'll start with one or two, and we'll get those working, and see how they go and gauge them. I'm telling you, man, there is more money in placing equipment and men on construction sites than there is in trying to build them or muck around trying to sell them. We should diversify our efforts because I've got some good ins in the construction industry, the unions for the placement of men, and the placement of machinery.[53]

Using fraudulent business details, the syndicate sought to arrange legitimate finance. Unlike the other frauds, they intended to make legal repayments. However, they needed to commit the initial fraud to secure the machinery finance, and from there to use the income from the first machinery to fund the acquisition of further machines; thus, as suggested by PF03b, the aim was to achieve a 'permanent income'.

Case 03 Discovery

As syndicate members were implicated in previous crimes, covert surveillance was undertaken and the actions of this syndicate as it relates to these crimes were identified.

5.4 Case 04

Case identifier	Case 04: Theft as an employee in union
Participant identifier	N04
Sources	New South Wales Police Force
Offence	27x176A *Crimes Act 1900* Director cheat or defraud 15x192H *Crimes Act 1900* Intention to deceive members or creditors by false or misleading statement of officer of organisation

[53] Case 03—LD Transcript

Case identifier	**Case 04: Theft as an employee in union**		
	5x351A(1) *Crimes Act 1900* Recruiting persons to engage in criminal activity		
Offender identifier	Identifier	Classification	Role
	PF04	Principal fraudster	Union general secretary
	AF04a	Associate fraudster	Procurement manager
	AF04b	Associate fraudster	Acting secretary
	AF04c	Associate fraudster	Printing company 1 co-proprietor
	AF04d	Associate fraudster	Printing company 1 co-proprietor
	AF04e	Associate fraudster	Printing company 2 proprietor
	AF04f	Associate fraudster	Spouse of PF04
	AF04g	Associate Fraudster	A union member who benefited from the scheme
	OT04a	Other	Chief financial officer (CFO)
	OT04b	Other	IT support

Case 04 was an investigation into the frauds of a high-profile union member. PF04a was the most senior employee at an Australian trade union that represented 35,000 members. He had been scrutinised over his election campaign spending, which caused considerable embarrassment for himself and a major Australian political party to which he was linked. To avoid future election spending scrutiny, he arranged for a corporate supplier (Company C04a) to provide him with supplementary credit cards from which he could spend without union, political or public oversight. Company C04a, owned by AF04c and AF04d, had lost a printing contract with the union several years earlier. PF04 offered them the chance to take up the contract again and, seizing on their desperation, arranged a meeting with them. PF04 convinced AF04c and AF04d, via Company C04a, to provide him, and AF04a whom he was having an extramarital affair with, with a supplementary American Express (AMEX) credit card, in return for recommencement of the lucrative union publication contract. An AMEX card was later supplied to another union member who was, at the time, a federal member of parliament, AF04g. To cover the expenditure of PF04, AF04a and AF04g, Company C04a submitted inflated invoices to the union. PF04 would approve the payment of each invoice using union-

issued cheques. The two-signatory corporate cheques, were countersigned by the union vice-president, who PF04 had convinced to pre-sign numerous blank cheques in the event of an emergency situation. This scheme ran from July 1998 until April 1999 when AF04c cancelled the AMEX cards because she became uncomfortable with the corrupt nature of this arrangement. This scheme defrauded the union of AU$74,025.32.

A second fraud occurred in the early 2000s when PF04 lied about a large amount of work that needed urgent attention. The Union Council unwittingly provided approval whereupon PF04 made representations that there was a large amount of work to be carried out, which the union could not do. PF04 then registered a limited company (Company C04b) as a trading name for his wife, AF04f. The alleged work involved the digitisation of years of union records, requiring the removal of staples and the scanning of paper records before destruction. While this work was initially undertaken by AF04f, it ceased shortly afterwards and between 1 June 2001 and 26 June 2009, PF04, via Company C04b, submitted 47 invoices totalling AU$620,326.67 for work never undertaken. The invoices submitted by Company C04b were processed by the union financial controller, OT04a, who was instructed to authorise the payment. During this time, PF04 never disclosed his connection to Company C04b, and as was the case with Company C04a, payment was made by union countersigned cheques.

In February 2003, PF04 arranged another meeting, this time with AF04e, the proprietor of another printing company (Company 04c). PF04 asked AF04e to quote on a printing job of 20,000 units for a union publication. AF04e was initially quoted AU$9 plus goods and services tax (GST) per unit, of which AF04e would receive AU$30,000 or AU$1.5 per unit in profit. PF04 instructed AF04e to further inflate the per-unit cost to AU$20 plus GST with the suggestion there would be a distribution of the excess proceeds from this fraud between PF04, AF04a and AF04e. Between 2003 and 2010, AF04e, with the approval of PF04, over-inflated invoicing for the union publication, business cards, lanyards and several other promotional items continued. The invoices, again paid by union cheques, were deposited by AF04e into a private bank account:

Over the next few days, he very carefully withdraws $9k, he might withdraw $27k, but does this on three separate occasions. So, in sums of $9k so as not to alert AUSTRAC [Australian Transaction Reports and Analysis Centre], then puts the money into a brown paper bag or an

envelope, then meets up with AF04a at a coffee shop where he gives her, her cut as well as PF04's cut of the money.[54]

Case 04 Discovery

The activities of this syndicate were initially revealed following a news article in the *Sydney Morning Herald*. This was followed by a public inquiry and finally, law enforcement officials became involved in 2011–12.

5.5 Case 05

Case identifier	**Case 05: Card skimming fraud targeting taxi patrons**		
Participant identifier	N05		
Sources	New South Wales Police Force		
Offence	1x351A *Crimes Act 1900* Recruiting persons to engage in criminal activity 2x193B *Crimes Act 1900* Knowingly deal with proceeds of crime 2x192L *Crimes Act 1900* Possession of equipment to make identification documents 2x192J *Crimes Act 1900* Dealing with identification information 2x192K *Crimes Act 1900* Possess identification information 1x192E Crimes Act 1900 Fraud		
Offender identifier	Identifier	Classification	Role
	PF05	Principal fraudster	Head of the syndicate
	AF05a	Associate fraudster	Co-offender
	AF05b	Associate fraudster	Mule, taxi driver who skimmed cards
	AF05c	Associate fraudster	Mule who withdrew funds from automatic teller machines (ATMs)

Case 05 was an investigation into the credit card skimming frauds of a Sydney-based criminal syndicate. Using handheld skimming devices, they recruited taxi drivers to skim the credit cards of business people and drunk taxi patrons. In the taxi, one of two skimming methodologies was used. In the first, they would ask for the customer's credit card to swipe

[54] Case 04 Detective N04 Transcript

using the electronic funds transfer at point of sale (EFTPOS) device fixed to the dashboard. They would deliberately drop the card at their feet and, while picking it up, swipe it through a card reader hidden under their seat. The position of the online EFTPOS device on the dashboard allowed the taxi driver to watch the victim enter their personal identification number (PIN), which they wrote down on a pad. The second methodology involved installing a more advanced EFTPOS terminal that recorded both Track 1 and Track 2 data and the PIN.[55] As noted by Detective N05:

> [a] businessman has a corporate credit card and doesn't generally check the credit card statement until the end of the month, so they have 1 month worth of using the credit card. Drunks don't see you skimming a credit card, they're either predisposed to falling asleep in your cab or being sick or whatever the trait is that the intoxicated person has. That is the specification that the head of the syndicate we looked at gave to his underlings.[56]

The taxi driver, AF05c, was paid AU$100 for each successfully skimmed card when he met with PF05 and AF05a, generally in a motel room. There, PF05 would connect the card reader to a laptop and download the skimmed card data. AF05a would then set up the card-cloning device, connect it to the laptop and, along with PF05, transfer the skimmed card data onto blank stock cards. AF05a would then write the PIN onto the corresponding card. AF05a then checked the first six numbers of each new cloned card on a website that listed IINs/BINs.[57] This let the syndicate members know which credit cards would be issued overseas, and therefore would be detected less quickly. AF05a and PF05 instructed AF05b to mark a 'T' on each of these cards, which means try more than once, as PF05 noted: 'when using these cards to get $500.00 out, then another $500.00 and then another $500.00'.[58]

Syndicate members then withdrew funds from the victim's accounts at ATMs. As Detective N05 noted:

> so what [PF05] would do was he would drive his car and he would pull over near an ATM and very quickly point to an ATM. They [AF05a and AF05b] would then pull up

[55] Track 1 data obtained from an EFTPOS card includes personal details, bank account, name, date of birth, BSB number, while Track 2 Data includes the customer's identification information as well as the algorithm which identifies the PIN (Gomzin, 2014).
[56] Case 05 Detective N05 Transcript
[57] Issuer Identification Numbers/Bank Identification Numbers.
[58] Case 05 Facts Sheet

> behind and two would get out of the car. Middle management [AF05a] would stand as look-out whilst the other bloke [AF05b] goes in and conducts the transactions.[59]

The funds were then divided up between PF05, AF05a and AF05b, and they would move onto the next series of crimes. The criminals sought to maximise their gain by withdrawing the daily limit from one card—say AU$2000—just before midnight, and then trying it again just after midnight to withdraw AU$4,000 from one account in a space of five minutes. However, this process was not random; it was planned. Evidence from the investigation suggested the fraudsters:

> targeted ATMs where there was no CCTV [closed-circuit television]. So, while at first glance it might just look like an opportunistic crime, there was a commonality amongst all the offences which gives rise to a belief that there is significant planning afoot in the commission of those offence.[60]

Case 05 Discovery

This crime was reported to the police by the victims.

5.6 Case 06

Case identifier	**Case 06: Card skimming fraud targeting service stations**		
Participant identifier	N06a male detective N06b female detective		
Sources	New South Wales Police Force		
Offence	2x193B(1) *Crimes Act 1900* Money laundering 2x93T(1) *Crimes Act 1900* Participate in criminal group 1x192J *Crimes Act 1900* Dealing with identification information 1x192e(1)(B) *Crimes Act 1900* Dishonestly obtain financial advantage by deception 1x192I *Crimes Act 1900* Possess equipment etc make identify information 2x256 *Crimes Act 1900* Making or possession of equipment for making documents		
Offender identifier	Identifier	Classification	Role
	PF06(1)	Principal fraudster	Organiser

[59] Case 05 Detective N05 Transcript
[60] ibid

Case identifier	Case 06: Card skimming fraud targeting service stations		
	AF06a(1)	Associate fraudster	Technician
	AF06b(1)	Associate fraudster	Technician
	AF06c(1)	Associate fraudster	Terminal importer
	AF06d(1)	Associate fraudster	Mule who allowed identity to be used by syndicate
	AF06e(1)	Associate fraudster	Scouted locations
	AF06f(1)	Associate fraudster	Mule placed in business

Case 06 was an investigation into the credit card skimming activities of another criminal syndicate.[61] Led by an international organiser who oversaw national organisers spread across five countries, the syndicate had at least four Australian sub-syndicates operating at the same time. Each sub-syndicate was run by a local organiser operating in major Australian cities and supported by international and local technicians who provided expertise to fraudulently tamper with EFTPOS devices that would be used in the frauds.[62] Each sub-syndicate, led by a local organiser, had technicians, cutters (mules who stole EFTPOS terminals)[63] and runners (mules who withdrew money from the victim's accounts). Together the Australian sub-syndicates of this larger international organised crime syndicate defrauded between AU$80 million and AU$100 million.

Using wireless EFTPOS terminals, the sub-syndicates targeted victims by placing the compromised EFTPOS devices in service stations and other businesses with high daily card volumes. Typically, sub-syndicates targeted businesses that would record more than 400 card transactions per day, to maximise their potential fraudulent gain. The method deployed by this syndicate evolved.[64] The first iteration involved covertly replacing normal EFTPOS devices

[61] Case 06 was an Australia wide crime undertaken by numerous local cells or syndicates with the activities of one cell represented in this case study. A random selection using a random number generator selected one cell over the others. The researcher did this as the sequence of events displayed across all syndicates were similar, and the researcher felt the inclusion of other narratives would provide no additional benefit within the scope of this thesis.

[62] Case 06 Detective N06 Transcript 'The [international] technician flew in with a pre-arranged cover story that he is the cousin of the international organiser, was schooled as to what to say to customs, what to expect, what not to bring, and all those things to avoid detection by law enforcement agencies, as well as to avoid any suspicion'.

[63] They did this by entering a shop, reaching over the counter, and cutting the EFTPOS cables before running off.

[64] Ghazi-Tehrani and Pontell (2021), found technology dependent crimes like phishing evolve in order to follow the money, but also to remain abreast of technological advancements.

with compromised EFTPOS devices, while also installing overhead pin-hole cameras to capture the PIN. When removed, they matched the PIN video footage to the Track 1 and Track 2 data captured in the compromised device. Because of some customers' tendency to hide their PIN entry, this resulted in only a 50% match. This methodology was also risky given the likelihood of being observed installing and removing the devices, coupled with the fact that when the compromised device was in place, the business was not receiving income. These challenges were overcome in some instances by bribing staff in the service stations to turn a blind eye to the installation and paying business owners for their lost income. There were instances of the sub-syndicate and business owners collaborating to install a mule at the service station who would be present when the compromised device was installed and then removed. The mule, usually an international student, would then leave the country so that the business owner had plausible deniability.[65]

The method evolved in response to technology updates. The second iteration of the scheme used pin-pad underlays—paper-thin electronic pads inserted under the EFTPOS terminal pin-pad. Wired to the magnetic stripe card reader, the pin-pad underlay provided increased accuracy when matching PINs to the Track 1 and Track 2 data. However, it was still not 100% because of matching issues. This methodology also removed the need to install pin-hole cameras, which reduced the potential for detection. The third iteration was triggered by technological advancements following improvements in Global System for Mobile Communication (GSM) technologies. It became possible for a sub-syndicate to remotely access EFTPOS devices and alter the software within the device. Track 1 and Track 2 data, along with corresponding PIN data, were captured and sent via GSM to the fraudster, situated outside the location of the compromised EFTPOS terminal. The fraudster could then encode the Track 1 and Track 2 data onto blank card stock and write the PIN onto a paper sticky dot on the other side of the card. These would then be offloaded to syndicate mules who would withdraw money from victim accounts without their knowledge. As Detective N06 noted:

> basically you go pay for your fuel, by the time you walk in, pay for it, by the time you get back to the car, drive home they've already got your card data your pin number, encoder, another card and withdrawing funds from your account before you get home.[66]

Case 06 Discovery

[65] Case 06 Detective N06 Transcript
[66] ibid

The principal fraudster PF06 had previously been identified as a lower-level criminal in a syndicate operating in Australia; however, he left the country before his detection. Several years later his return to Australia was detected by law enforcement who observed his activities before arrest.

5.7 Case 07

Case identifier	**Case 07: Debt factoring fraud**		
Participant identifier	N07		
Sources	New South Wales Police Force		
Offence	5x178BA *Crimes Act 1900* Obtain benefit by deception 9x192E Crimes Act 1900 Fraud		
Offender identifier	Identifier	Classification	Role
	PF07	Principal fraudster	Proprietor of panel beating company
	AF07a	Associate fraudster	Co-proprietor of panel beating company
	AF07b	Associate fraudster	Worked for an organisation with a large vehicle fleet

Case 07 was an investigation into a debt factoring fraud. PF07 was the co-owner of a panel beating company with her husband AF07a and was supported in this fraud by AF07b, a manager at a Sydney-based organisation with a large fleet of vehicles. Debt factoring in the automotive panel beating industry describes a process to recover the costs of repairs from insurance companies on time. Panel beaters routinely shift the burden of collecting insurance costs to a specialised debt factoring company in return for a percentage fee on the monies owed. The debt factoring company then recoups their costs from the insurance company. This allows the panel beater to raise working capital to put back into the business.[67]

The company owned by PF07 and AF07a was awarded a small contract to undertake vehicle body repairs by the company for which AF07b worked. Faced with financial difficulties, PF07

[67] As an example of how this works, the smash repairer held $100,000 on their debtor's list; they approached a debt-factoring company who would then offer to pay them $95,000 and in turn the debt-factoring company would keep the remaining $5,000 as their payment once they had collected on the debt, typically at the end of a 90-day period.

submitted a fraudulent debt factoring request to a victim debt factoring company. To support this, PF07 fraudulently altered contracts of work and bank statements to convince the victim organisation that her company had sufficient upcoming work. The result of this initial fraud was twofold: first, she received a cheque from the debt factoring company; and second, she knew that at the end of the 90-day period the initial victim organisation would be expecting payment from the insurance company. Knowing this would not occur because the contracts were fraudulent, PF07 submitted a second debt factoring request to another debt factoring company with the intention that she would use a second lot of funds to pay off the first debt factoring company. Given the debt factoring process attracted fees, and that PF07 spent some of the funds on herself, each time she submitted another fraudulent debt factoring request, the sums involved grew.

PF07 needed to provide proof to the debt factoring companies that she had sufficient contracts of work to sustain the continually increasing value. While it was not known how the initial approach occurred, the value of AF07b to this syndicate became apparent at this time. Given his position within a corporation with many trucks, AF07b was able to backstop the claims being made by PF07 as to the number of vehicles her company was repairing every week. AF07b also began taking executives from debt factoring companies on site visits where he would point out one truck after another that he claimed had either been repaired or needed to be repaired by PF07 and her company.

Case 07 Discovery

One of the debt factoring companies engaged by PF07 identified that the bank accounts from which they were receiving funds were the same as those of PF07's company. The payments should have been coming from the insurance company. Consequently, the debt factoring company called in their auditors who reported the matter to the police.

5.8 Case 08

Case identifier	**Case 08: Fleet vehicle procurement fraud**
Participant identifier	N08
Sources	New South Wales Police Force
Offence	10x249B *Crimes Act 1900* Corrupt commissions or rewards 1x192D *Crimes Act 1900* Obtaining financial advantage

Case identifier	Case 08: Fleet vehicle procurement fraud		
Offender identifier	Identifier	Classification	Role
	PF08	Principal fraudster	Fleet manager with the victim organisation
	AF08a	Associate fraudster	Consultant with Toyota dealership
	AF08b	Associate fraudster	Individual who allowed his bank account to be used as part of the fraud
	AF08c	Associate fraudster	General manager at a fleet service company
	AF08d	Associate fraudster	CEO at a fleet service company

Case 08 was an investigation into procurement fraud. AF08a was a consultant for a vehicle wholesaler who had set up a procurement deal between the victim organisation employing PF08 and the fleet service company at which AF08c and AF08d worked. Under normal circumstances, the victim organisation replaced its vehicle fleet on an ongoing basis. Their procurement manager, PF08, would approach a fleet service company and work out a contract to supply the vehicles to the victim organisation. The fleet service company would then source vehicles from a vehicle wholesaler who would slightly increase the wholesale price of each vehicle, which is how such businesses make their money. The fleet service company would then supply the vehicles and, in the contract, they too would increase the price slightly, which is how this business makes their money. Under this model, the procurement manager only received a salary from the victim organisation.

The fraudulent scheme began with an initial legal agreement between AF08a, the consultant for the vehicle wholesaler, and AF08d at the fleet service company. There was an initial agreement that the fleet service company would pay AF08a a lawful commission of AU$30 per vehicle, per month. However, when PF08 at the victim organisation became aware he wanted a cut of the payments, as Detective N08 noted:

> [AF08a] knew that [PF08] was not entitled to any payment and understood that the payment was going to [PF08] and not [the victim organisation]. [AF08a] knew that if he didn't make the payment to [PF08], he could influence [victim organisation]

objecting to the payment of any commission or the terms of the [victim organisation] deal.

AF08c then suggested a one-off payment of AU$1,000 per vehicle as a more efficient approach than the per vehicle, per month model. The fleet service company notified the vehicle wholesaler how many vehicles had been placed with the victim organisation. The vehicle wholesaler then invoiced the fleet service company. The vehicle wholesaler would keep AU$250 of the commission per month, with the rest paid directly to AF08a. However, in line with instructions from PF08, AF08a let the commission for PF08 accumulate until PF08 provided instructions on where and how to make any funds available. Eventually, the vehicle wholesaler became increasingly concerned with the corrupt nature of the payments and withdrew; they did this by selling their interest in this deal to AF08a for AU$80,000. From that point on, AF08a invoiced the fleet service company directly.

At the end of the initial commercial lease, the fraudsters were required to alter the method in which the payments were made because the new commercial lease was subject to increased oversight. Thus, to retain the corrupt payments scheme, the fraudsters reduced the per-vehicle payment in stages from AU$1,000 to $720 to $560 and finally to $500, and altered the method of payment. Using a shelf company, they invoiced the fleet service company for a fictional range of services linked to the pre-inspection supply of the vehicles, the cost of which was buried in complex language and figures within the overarching contract between the victim organisation and the fleet service company. Throughout this process, PF08 continued to demand his corrupt payments, funded by his employers, even to the extent of demanding his 50% share of the corrupt payment be increased to 70%, to which the other parties agreed to ensure continuation of the broader scheme. This process of criminal commissions continued with a series of fleet-flips taking place, which is when the entire fleet is replaced with another vehicle type.

Case 08 Discovery

This fraud was detected following a tip-off by a whistle blower.

5.9 Case 09

Case identifier	Case 09: Theft by a telecommunications company employee		
Participant identifier	N09		
Sources	New South Wales Police Force		
Offence	35x178BA *Crimes Act 1900* Obtain benefit by deception 29x192E Crimes Act 1900 Fraud 3x157 *Crimes Act 1900* Embezzlement 2x192G *Crimes Act 1900* Intention to defraud by false or misleading statement		
Offender identifier	Identifier	Classification	Role
	PF09	Principal fraudster	
	AF09	Associate fraudster	

Case 09 was an investigation of employee fraud against a telecommunications company and its employees. PF09, a retired detective, worked as fraud investigations manager for a telecommunications company. His manager and accomplice, AF09, was also a retired detective. The frauds committed by PF09 and AF09 are divided into two categories: those committed against the victim organisation; and those committed against staff.

PF09's procurement crimes centred on his manipulation of the victim organisation's procurement systems and processes. PF09 identified customer accounts that had been subjected to identity takeover attempts, which if successful allowed other fraudsters to order new iPhones. He convinced the procurements team to forward the phones to him so he could affect something called a 'controlled delivery'.[68] Instead, PF09 gifted the iPhones to members of his local National Rugby League (NRL) club who were not aware of this fraudulent activity. Doing so allowed PF09 to ingratiate himself with NRL club players and notables as a generous benefactor. As a result, he was invited to private events, while his children ran onto the field with the NRL players before games and visited them in the changing rooms. In this way, PF09 became a prominent figure in the NRL club's supporter community.

PF09 also used his role within the victim organisation to copy and refine the crimes of those he was tasked with investigating. As Detective N09 noted: 'I had used some of those facts sheets he had prepared for [former staff members he had investigated] because he was

[68] Controlled delivery, from a law enforcement perspective describes an action undertaken by law enforcement to intercept a package, generally containing drugs, and then allowing its delivery to the intended address with the intention of identifying participants.

committing offences, he was learning what they were doing, and he was doing the same thing'.[69]

The next series of crimes committed by PF09 and AF09a centred on the extortion of monies from employees subject to internal fraud investigation. During the investigation, PF09 and AF09 identified potential targets, usually of Asian background, and extorted the value of their frauds from them. In these crimes, PF09 and AF09 prepared a prosecution brief of evidence for each staff member who had stolen from their employer, ready to be submitted to the NSWPF. However, before sending it to the police, PF09 and AF09 approached each staff member and advised them a police prosecution was not necessary if the staff member paid back the value of their fraud to PF09 and AF09. The monies paid to PF09 and AF09 were always directed to be in cash, always made in person and never returned to the victim organisation; instead PF09 and AF09 divided them between them.

Case 09 Discovery

The activities of PF09 and AF09 were uncovered when the family of a former employee refused to allow their daughter to meet PF09 and AF09 with a cash payment of AU$12,000. As a result, PF09 finalised the prosecution brief of evidence and submitted it to the NSWPF. At a later stage, an allegation was made in a separate jurisdiction about the activities of PF09 and AF09, whereupon the victim organisation was contacted. The victim organisation then undertook a discrete internal review and identified several instances where PF07 and AF07 had deviated from standard human resources practices.

5.10 Case 10

Case identifier	**Case 10: Accounting fraud**		
Participant identifier	N10		
Sources	New South Wales Police Force		
Offence	26x192E (b)(1) *Crimes Act 1900* Fraud 20x178BA (1) *Crimes Act 1900* Obtain money by deception 2x 78A *Crimes Act 1900* Fraudulent misappropriation of monies collected or received/failure to account		
Offender identifier	Identifier	Classification	Role

[69] Case 09 Detective N09 Transcript

Case identifier	Case 10: Accounting fraud		
	PF10	Principal fraudster	Sole fraudster
	OT10	Associate fraudster	Former client and fraudster

Case 10 was an investigation into an accounting fraud. PF10, an accountant, ran a successful accountancy business. OT10, a former client, declared bankruptcy, owing PF10 AU$150,000. Unlike other crimes in this study, PF10 was both the principal fraudster and a victim of another fraud committed by OT10.[70] A short time after declaring bankruptcy, OT10 approached PF10 offering him an opportunity to recoup his money. As PF10 noted to police:

> I think that was in the February of 2006 when we had a meeting, I mean [OT10's] a nice enough guy, we had a bit of a meeting and we talked about, how would you like to get your money back? And I said, 'well that would be great'.[71]

PF10 went on to describe the investment OT10 offered him:

> we talked about people that he [OT10] had dealings with overseas that would be able to get a return to investors of about 10 per cent per annum and I would get some form a brokerage. So, what happened was I had only recently sold my principal place of residence in Karelia and I had approximately AU$100,000 and it started off in dibs and drabs in terms of handing him money[72]

By the middle of 2006, PF10 had not seen returns, so he asked for the money back; however, 'over a period of time there were various dates or that were actually proposed in terms of the funds would be able to be returned, those dates came and went and there was always some issue'.[73] The fraudsters with PF10's monies continued to come up with numerous excuses as to why the funds were not being returned:

> We've attempted to send money and then the money's bounced back, our computer system's been sabotaged. They need more money for software or computers, whatever because my belief was and still is that money was being sent to a bank and that bank for, for all intents and purposes was or is in New York in the States.[74]

[70] PF10, according to Goldstraw-White (2011) was a pressured actor.
[71] Case 10 PF10 Transcript
[72] ibid
[73] ibid
[74] ibid

Overall, PF10 displayed a degree of naivety, which was demonstrated when he tried to explain how he communicated with the supposed investors:

> the way the communication works is I received a text message. The banks can have their own computer systems and they have their own means of communication and my understanding of it is that they securely send messages in terms of, we need this amount to invest, or we've had a problem here or whatever, so we would receive text messages requesting certain funds at certain times. And that text message went through a series of people it came from the people in the United States to a person in Australia, from the person in Australia to OT10, from OT10 to me.[75]

Once PF10 had exhausted his funds, and to meet the increasing demands from OT10, he began to steal from family and clients.[76] PF10 conceptualised his theft from family and clients, not as fraud or theft, but as a legitimate investment that would provide 10% returns, thus allowing him to get more money to the United States and free up his funds. He stated:

> [my clients] wanted to invest their funds, what happened was the share market was all over the place, so I say, I'll get you a 10 per cent return, and that's basically how it worked. So, [my clients] wrote me cheque, gave me authority to operate on their account so yeah that's how it worked.[77]

However, PF10 was not simply an unsuspecting victim; he also demonstrated a level of sophisticated planning linked to the theft of his clients' funds. For example, he purchased and used several mobile phones in fake names so people could not track his communication with OT10, which is contrary to the impression given that he was a victim in this matter.

Case 10 Discovery

The activities of PF10 were finally detected by his clients who had not received the promised returns. In some instances, his clients contacted their banks to trace their funds, finding they had not been sent to where PF10 had claimed they had. While in others the Australian Taxation Office had contacted PF10's clients advising them that they had not supplied the taxation authorities with returns over several years, despite them transferring money to PF10 to meet annual taxation commitments.

---

[75] ibid

[76] The way PF10 interacted with OT10 was interesting because it appeared that while he suspected, or at least considered that this might be a scam, he then almost as quickly dismissed it and considered it a legitimate enterprise what was at worst, shady.

[77] Case 10 PF10 Transcript

5.11 Case 11

Case identifier	Case 11: Land valuation mortgage fraud		
Participant identifier	N11		
Sources	New South Wales Police Force		
Offence	23x193B(3) *Crimes Act 1900* Recklessly deal with proceeds of crime 5x193B(3) *Crimes Act 1900* Attempt to recklessly deal with proceeds of crime		
Offender identifier	Identifier	Classification	Role
	PF11	Principal fraudster	Head of the syndicate
	AF11a	Associate fraudster	Forger
	AF11b	Associate fraudster	A former employee of the victim organisation, and provided the syndicate with an introduction to the insider
	AF11c	Associate fraudster	An insider with the victim organisation

Case 11 was an investigation into mortgage fraud.[78] PF11 was a career fraudster who considered himself a property developer. AF11a was a career fraudster and an expert forger. AF11b was a former employee of the victim organisation who had previously been dismissed for similar crimes and was an associate of PF11. AF11c was a mobile lender with the victim organisation and had worked previously with AF11b.

A process known as land resumption was the basis upon which this crime was built.[79] In a remote western NSW township, many vacant undeveloped residential blocks were subject to council rate defaults. When rates debt exceeds the value of a property—in some instances as little as AU$1,000 for an 800 m^2 block—councils can enact a land resumption process to recoup the value of the rates and return the property to state ownership. In the current case, at

[78] Nguyen and Pontell (2010) contended mortgage fraud was an intentional act or omission that led others to act on the information in the application in a way that was detrimental to their own interests.
[79] Land resumption described a situation where government at a Local, State of Federal level is able to reacquire some or all of a private individual's land for specified purposes (NSW Land Registry Services, 2021).

subsequent auction, these low-value properties were purchased by a company that specialises in purchasing and on-selling low-value developed and undeveloped residential blocks.

PF11 and AF11a purchased the title deeds to 23 of these properties for AU$5,000 each. They subjected each title deed to a series of non-existent sales over several months using fictitious vendor details, all of which were forged by AF11a. Each fictitious sale increased the value of the block to the point that the NSW Land Registry Service records revealed the 23 properties were now valued at between AU$245,000 and AU$285,000 each.

PF11 recruited AF11b who had a background in the residential mortgage market. AF11b provided the syndicate with recent experience and access to several of the victim organisations' procedural documents used during the mortgage application process. AF11b then introduced AF11c—who was still working within the victim organisation—to the syndicate.

PF11, with the assistance of AF11b, completed numerous mortgage loan applications based on the fraudulently inflated value of the undeveloped residential blocks. Subsequently, 28 fraudulent mortgage applications were submitted by AF11b to AF11c at the victim organisation. Knowing these frauds relied on falsified land values, and that a mortgage valuation inspection would reveal the fraudulent nature of the land values, AF11c needed to devise a method for avoiding detection. Detective N11 described the actions of AF11c in devising a way around the controls:

> on day one he puts a series of entries into [the victim organisation's] computer and it generates a [requirement for physical inspection] valuation report. Then later that day he changes one or two of the answers for the same property and it generates [the same] report. So over 3 days, he puts in seven different combinations and the seventh one is the first time he gets 'no external valuation required'. Then every loan after that is done in the same way. So basically, he worked out the system, which he logs on, but he never finalises each time because he doesn't get the outcome that he wants. He goes back, thinks about it, has another crack and then eventually on attempt seven he got it and then each one thereafter, it's one attempt to get the same answer.

Using this method, in 8 months, the syndicate submitted a total of 28 loan applications that resulted in the disbursement of AU$4,917,150.00 via accounts managed by AF11b. The funds were then transferred on for the benefit of the syndicate.

Case 11 Discovery

The activities of this syndicate were finally detected by the NSW Land Registry Services who queried an apparent property boom in the remote western NSW township.

5.12 Case 12

Case identifier	**Case 12: Superannuation fraud**		
Participant identifier	N12		
Sources	Australian Federal Police		
Offence	1x134.2 *Criminal Code Act 1995* (Cth) Obtain financial advantage by deception 1x400.3(1) *Criminal Code Act 1995* Money laundering		
Offender identifier	Identifier	Classification	Role
	OT12a	Organiser	International organiser
	PF12a	Principal fraudster	Provided connections to a domestic criminal network
	PF12b	Principal fraudster	Met with A01IO overseas where it is believed this individual received instructions relating to the scheme
	AF12a	Associate fraudster	Managed crime implementation and did call-back procedure
	AF12b	Associate fraudster	Telecom technician
	AF12c	Associate fraudster	An insider at the victim organisation
	AF12d	Associate fraudster	Connected PF12a with AF12h
	AF12e	Associate fraudster	Connected PF12a with AF12c
	AF12f	Associate fraudster	Holder of Greek bank account through which funds were laundered
	AF12g	Associate fraudster	Holder of Swiss bank account through which funds were laundered
	AF12h	Associate fraudster	Laundered funds on casino ship
	AF12i	Associate fraudster	Laundered funds on casino ship

Case identifier	Case 12: Superannuation fraud		
	AF12j	Associate fraudster	Met with A01IO overseas where it is believed this individual received instructions relating to the scheme

Case 12 was an investigation into a superannuation fraud. The syndicate, led by PF12, stole AU$150,000,000 from an Australian superannuation fund held by the victim holding bank, which was managed by a global fund's management company. Under normal circumstances, the fund's management company instructed the holding bank to move funds around as part of its investment strategy and these instructions were delivered via secure facsimiles between the two financial institutions. In the months leading up to the crime, several funds transfer request documents were stolen by AF12c. Using these, other members of the syndicate forged a legitimate-looking funds transfer request document. On the day of the fraud, AF12a and AF12b entered a telephone exchange in the Sydney central business district. AF12b hacked the exchange mainframe, enabling AF12a to send a funds transfer request document to the victim bank, requesting the transfer of AU$150 million to the four nominated bank accounts. The funds transfer request sent by AF12a was supposed to appear, to the victim bank, as having originated from the fund's management company. However, for an undisclosed reason, the funds request could not be sent via the hacked telecommunications line prepared by AF12b. Instead, AF12a sent the funds request via another telecommunications line located within the exchange. The funds request received by the victim bank directed that the funds be split and transferred across four separate accounts: AU$20.6 million and AU$30.4 million to two bank accounts in Hong Kong; AU$26.7 million to a bank account in Switzerland; and AU$71.9 million to a Greek bank account. AF12a then phoned the victim bank on a hacked phone line so it appeared he was calling from the fund's management company, to effect the 'call-back' procedure.[80] AF12a pretended to be a staff member from the fund's management company, a real person who had had his identity stolen, in finalising the fraud. AF12a then spoke to AF12c, the insider at the victim bank, and together they went through the security procedure and the funds were transferred overseas.

Case 12 Discovery

[80] Case 12 Detective N12 Transcript: 'A call-back procedure was a security procedure implemented to ensure the credibility of the requested transfer before it being actioned. Despite the process normally being the receiving institution would make the call, it was not uncommon for the sending institution to occasionally instigate the process, which is outside of normal operating policies.

The AU$71.9 million transferred to a Greek bank account was in the name of AF12f. However, the deposit information listed the account as AF12f 'Ltd'. Staff at the Greek bank contacted the victim bank on the next business day asking them to resend the transfer request, this time without the 'Ltd' suffix. This alerted the victim bank to the fraud. The AU$30.4 million arrived at the Hong Kong account where it was immediately withdrawn by AF12h and AF12i, who boarded a Hong Kong-based gambling ship, where the money was laundered as gambling chips. The AU$20.6 million arrived at another Hong Kong account. However, by the time PF12b arrived from Australia to withdraw the money, the accounts had been frozen. The AU$26.7 million arrived at the AF12g account, but by the time AF12g attempted to withdraw the funds, they had been frozen.

5.13 Case 13

Case identifier	**Case 13: Insider trading**		
Participant identifier	N13		
Sources	Australian Federal Police		
Offence	1x142.2(1) *Criminal Code Act 1995* Abuse of public office 1x372.1A(1) *Criminal Code Act 1995* Dealing in identification information that involves use of a carriage service 1x1043A *Corporations Act 2001* (Cth) Prohibited conduct by person in possession of inside information 1x1311 *Corporations Act 2001* General penalty provision 1x400.4(1) *Criminal Code Act 1995* Intentionally dealing in proceeds of crime		
Offender identifier	Identifier	Classification	Role
	PF13	Principal fraudster	Trader
	AF13	Associate fraudster	Insider

Case 13 was an investigation into an insider trading scheme. PF13 worked as a foreign exchange trader for a large Australian retail bank and AF13 worked for an Australian Government department. The fraud involved spot trading on 'FX margin contracts', commonly referred to as news trading.[81] Following the release of Australian Government data, Australian and other global financial markets would often fluctuate in value, as Detective N13 noted:

[81] News trading is a strategy of placing trades either in anticipation of, or in response to economic data releases (Foucault, Hombert, & RoȘU, 2016).

> it's called 'news trading' and big companies do it. They generally do it with computers and algorithms, so they generally get a pretty good result and it's very quick. So, it's not uncommon to see large volumes of trade at those particular times.

PF13 and AF13 had known each other since high school:

> they used to get together every year for a mutual friend's birthday but at some stage, they started talking about what AF13 does at the [government department] and what area he's in. I think he'd just moved into an area that was providing sensitive data or analysing sensitive data for release and PF13 had moved into a foreign exchange area in [the bank]. His area wasn't to do with contract trading and that sort of stuff, it was more to do with buying and selling foreign currency for businesses. But in that role, he was able to get market snapshots they sent out to everyone of what the foreign currency is doing around the world, what economic news was coming up, who's releasing it, forecasts like internal forecasts only for [bank] people and then your global forecasts that are going on. It was all to help [PF13] in his job, but I think it was getting access to that information and then speaking to AF13 and finding out what he was doing with the [government department] and putting 2 and 2 together is what really sparked this notion of 'hey, I've got an idea of how I think we can make some money'.[82]

AF13 had the data, and PF13 had the knowledge to set up the trading accounts and the foreign exchange markets. PF13 used the pre-release data from AF13 to identify where he should place his trades to extract the highest possible returns from the rise and fall in the markets. They targeted these systems because, according to Detective N 13: 'firstly it was unregulated, or he thought it was unregulated and he thought that he wouldn't get exposed. Second, he could get access to the tipping information that he needed'.[83] Ultimately, this insider trading scheme resulted in a gain of AU$7million for PF13. AF13, meanwhile, was only expecting the scheme to net the pair AU$200,000, as described by Detective N13:

> part of their agreement was that PF13 would do all the trading in his name, all the money would go through his bank accounts and he'd pay tax on any winnings and then they'd split the winnings 50:50. So the agreement made was that they'd do it for 12 months or

[82] Case 13 Detective N13 Transcript
[83] ibid

> up to $200,000 in total. So AF13 was expecting a profit of $50,000 once you pay 45–50% tax and then whatever the $100,000 left, they'd split 50:50.[84]

However, PF13 was deceptive by operating side trades of which AF13 had no knowledge, which was part of the reason why this insider trading scheme was detected. As Detective N13 noted of PF13, 'He was definitely the manipulator and to keep AF13 committed to fulfilling the original agreement of doing it up to $200,000 or 12 months', he hid the success of his trades to keep AF13 supplying the insider information.

Case 13 Discovery

This crime began to unravel for the syndicate when the big four banks began to complain to the regulators that an individual trader was beating them at their own game and they were losing significant amounts of money. However, while they suspected something was not right, neither the banks nor law enforcement knew how PF13 and AF13 were doing it. It was not until AF13 left his burn phone at home on a trip to see PF13, which forced AF13 to use his mobile phone, that police were able to link the two.

---

[84] Case 13 Detective N13 Transcript

Chapter 6: Tradecraft—Access in Financial Crimes

Understanding the reason for variation in the implementation of fraudsters' tradecraft is important in the study of how financial crimes are committed. To identify variation and the causal factors that trigger these differences, it is necessary to devise a strategy that focusses on the distinct stages of the criminal process. In this chapter, that distinct stage is access. The focus on access—one of the three temporal stages of the ALPi Model—provides an insight into how access varies and what impact, if any, this will have on how the crime unfolds.

The first of three chapters aligned to the ALPi Model, this chapter acknowledges that access occurs in more ways than can be covered herein. The chapter provides an analysis of variation in how access was achieved across the cases. The central determinant of differences in nearly all cases was the proximity of the principal fraudster to the financial system. As the key variable in this thesis, proximity accounts for variation in how and why fraudsters approach their crimes. The chapter reveals a connection between knowledge acquisition and access; for example, in the insider cases, the fraudsters tended to gain access to financial systems and then learn how they operated; whereas outsiders tended to acquire knowledge before gaining access to the target financial system, which highlights variability in the nature of the offending process.

This chapter is split into two sections—access by the insider and access by the outsider—drawing on the case data outlined in Chapter 5 from two police jurisdictions. The similarities and differences predicated primarily around the proximity variables made it possible to group the themes that arose from the data in new ways, see Table 7. This made it possible to shed light on the 'how' of fraud on which this thesis focusses.

The first section of this chapter focusses on access and insider opportunities. Specifically, it draws together themes identified in the case management files. The second section focusses on access and outsider opportunities. In the absence of legitimate insider

positions of trust, principal fraudsters who were classified as outsiders could not rely on traditional avenues usually available to insiders. Outsiders instead demonstrated increased guile and cunning in their efforts to achieve the same level of access as their insider counterparts.

Table 7

Case Status—Insider/Outsider Cases

Insider/outsider status					
Case number	Crime type	Principal fraudster—insider	Associate fraudster—insider	Principal fraudster—outsider	Associate fraudster—outsider
01	Procurement fraud		X	X	
02	Account takeover			X	X
03	Mortgage fraud			X	X
04	Theft as an employee	X	X		X
05	Credit card skimming			X	X
06	Credit card skimming			X	X
07	Debt factoring			X	X
08	Procurement fraud	X			X
09	Theft as an employee	X	X		
10	Accounting fraud	X			
11	Mortgage fraud		X	X	X
12	Superannuation fraud		X	X	X
13	Insider trading	X			X

X – indicates a positive correlation between the χ-axis and the γ-axis

6.1 Access and the Insider

Conventional wisdom often yields broad statements about malicious insiders, for example, the belief that malicious insiders are a relatively rare phenomenon (Australian Government, 2016, p. ii; Gray, 2013, p. 534). It also suggests malicious insiders are likely to have shown loyal service before abusing their position of trust, and even that insiders manage their fraud to ensure it does not stand out (Carnegie Mellon University, 2012, p. 14). Viewed from these perspectives, it is easy to assume one insider is likely to be much like another. Following this line of reasoning then, the tradecraft displayed by individual fraudsters would largely be the same—provided of course there was similar access, knowledge and criminal intent.

A 2016 commissioned report identified the trusted insider as 'a real and enduring risk' (Australian Government, 2016, p. ii). Indeed, the ease with which insiders can use their 'knowledge of and access to proprietary systems [coupled with] their ability to bypass security measures through legitimate means' adds weight to perceptions that malicious insiders are likely to be highly similar in both their preparatory and substantive criminal actions (Carnegie Mellon University, 2012, p. 1). Such assumptions, whether grounded or mythical, are likely to influence how those charged with the responsibility of protecting organisations limit the risk of exploitation by malicious insiders.

To determine the extent to which a fraudster's status as an insider shapes the implementation of their tradecraft, it is necessary to establish the extent to which insiders share features. While logic suggests that, by virtue of their occupational position, insiders already have the required access (Carnegie Mellon University, 2012), this ignores the fact that not all insiders have access to all parts of a victim organisation.[85] Therefore, assumptions

[85] An example of this might be seen in a hypothetical example where an insider fraudster has access to one system, but not another because of separation of duties (SOD) controls within the organisation. Therefore, obtaining access to a restricted system would allow the completion of their crime.

based on the premise that all insiders can access every part of an organisation overlook the presence of internal controls (Appiah, 2015). The remainder of this section explores the variation in cases where the principal fraudsters were insiders.

6.1.1 From Opportunistic to Planned

The data suggest that while opportunity was a common explanation for the initiation of crime, there was evidence of significant planning across insider cases. Opportunity is a frequent topic of exploration in the criminological literature and is often referred to as a causal explanation for financial crime (Benson & Simpson, 2018; Dellaportas, 2013; McGrath, 2020). As identified in Chapter 3, there are three broad types of insider: the unintentional insider (Australian Government, 2016), the opportunistic insider (Goldstraw-White, 2011) and the malicious insider (Carnegie Mellon University, 2012). The data in Table 8 show that three of five cases were classified as opportunistic as the fraudsters reacted to unplanned opportunities.[86] However, the continuation of offending in these cases suggests that the argument that opportunity alone was present in these cases misrepresents reality. Instead, increases in planning were observed across all three cases, shifting them from opportunistic frauds at the outset to something more closely resembling the concept of the planned and malicious acts of an insider (Carnegie Mellon University, 2012). As Detective N08 contended ‘it was an opportunity that started it; then it evolved into a planned crime’.

[86] Case 08 / Case 09 / Case 10

Table 8

Insider Case Access Characteristics

	Insider opportunity							Other	Insider motivation			Characteristics of victim suitability		
					Malicious insiders									
Case	Routine daily activities	Specialised access positions	Unintentional insiders	Opportunistic insiders	Seeks opportunities within own organisation	Pre-employment subversion	Post-employment subversion	Outsider critical to insider crimes	Primary motivation	Secondary motivation	Tertiary motivation	Familiarity	Lack of controls	Access
04	X	X			X	X	X	X	M	TL		X		X
08	X	X		X	X		X	X	M				X	
09	X	X		X	X				EC	M				X
10	X	X		X	X				TL	M		X	X	X
13	X	X			X		X	X	M	SS				X

Note. * TL, threat of loss; M, money; EC, ego challenge; SS, sense of superiority

X – indicates a positive correlation between the χ-axis and the γ-axis

Opportunity, however was not evident in all cases. In two of the five,[87] there was evidence that some frauds were maliciously planned from the outset. The importance of this is that, unlike in Cases 08, 09 and 10, the absence of an initial opportunity did not deter the principal fraudsters in Cases 04 and 13; instead, they actively set out to engineer the opportunity themselves. For example, Detective N13 observed:

> it's a pretty strong mixture of planning and development, it's almost like research and development. [It was like] having the required knowledge of the financial systems through university and then entering that space through work. Then it was about identifying how to beat the system and then it was about working out what was needed to beat the system. Then it was about trial and error, then planning and then putting the plan into action.

Indeed, the level of effort required in these cases to engineer the so-called opportunity was significant. In Case 04 involving theft by a union employee, the principal fraudster PF04 arranged multiple meetings with a potential printing supplier, asking them to quote on corporate printing jobs on behalf of the victim organisation. The supplier quoted AU$9 + GST per unit but was told by PF04:

> We've been paying much more than that for the book. It wouldn't look good for me if it only cost $9 per book. We've been paying much more than that. The auditors might ask why we've been paying so much. It could be questioned. What if you make it $20 per book? You'll get the job, but we have to put the price up from what you've quoted. We'll split the difference.[88]

In addition to identifying that not all frauds are opportunistic from the outset, this case provides an example of pre-employment subversion (Walton, 2006). In this instance, PF04

[87] Case 04 / Case 13
[88] Case 04 Statement-AF04e

recruited AF04d, the printing supplier, to a criminal enterprise before the contract was signed. Thus, the supplier was likely to be more loyal to the principal fraudster than to the victim organisation. Similarly, Case 13, the insider trading fraud, provides an example of post-employment subversion (Walton, 2006). This time the principal fraudster approached a former schoolmate and subverted him to his criminal endeavour. In this instance, rather than working for the victim organisation, the subverted insider worked for a second organisation that dealt with sensitive government information that, in the right hands, could be used to manipulate financial markets to the benefit of the principal fraudster.

6.1.2 It's Part of 'My Job'

Linked to the exploration of opportunity in the previous section is the criminological truism that the opportunity to offend commonly arises in settings where the motivated offender encounters a suitable victim in the absence of a capable guardian (Cohen & Felson, 1979). In workplace settings, this points to the insider with criminal intent who accesses a financial system and, using their awareness of that financial system's controls, circumvents them. As outlined out in Table 7, access derived directly from the insider's daily routine activities were present in all insider cases.[89] This section draws together the three components of routine activity theory in an analysis of the insider data.[90]

6.1.2.1 Motivated Offender

The insider data analysed in this section reveal a wide variety of motivational factors at play. In addition, the data identify a common tendency for the motivations of insiders to evolve throughout their fraud events. Table 8 shows that the first aspect of Cohen and Felson's (1979) hypothesis—the motivated offender—was evident in the insider case data. Setting aside the obvious fact that all fraudsters are motivated, and Cohen and Felson's

[89] Case 04 / Case 08 / Case 09 / Case 10 / Case 13
[90] See (Cohen & Felson, 1979)

(1979, p. 589) hypothesis downplays the importance of motivation, the data suggest that motivation is not a static phenomenon. Instead, the data provide evidence that a fraudster's motivation evolves with time, as Detective N04 pointed to:

> In [Case 04] it was greed, I think in the mid-2000s he was on AU$350,000 per annum, and he was not satisfied with that amount of money. [Later] he was committing this crime to obtain extra money. His wife and children became accustomed to living this high life; dad is earning all this money, and then there is this pressure to keep this up.

In contrast, Case 09 involving theft by a telecommunications company employee, depicted a fraudster who was initially driven not by greed but by narcissistic tendencies.[91] In this case, the principal fraudster PF09 sought to figuratively rub shoulders with the highfliers of a prominent Australian sporting code. As Detective N09 described, the principal fraudster's motivations were initially narcissistic: 'He wanted to be the nexus of the [sporting code], he wanted to rub shoulders with the stars, and he just wanted to be a heavy hitter, wanted everyone to like him'.

In this case, PF09 engaged in an array of criminal offending to attain his goals. For example, he was the investigations manager at an Australian telecommunications organisation where he had the responsibility of leading a department of fraud investigators that investigated staff members and account holders that sought to defraud the organisation. On occasions when the organisation identified a potential fraud involving the theft of iPhones, PF09 would manipulate internal systems and divert the iPhones that had been stopped before dispatch. He did this via the false claim that he would use those iPhones as

[91] This finding was contrary to the common perception that greed is the primary motivator (Ghazi-Tehrani & Pontell, 2021).

part of the ongoing investigation. Instead, he simply took the iPhones and passed them on to high-profile figures in the sporting code to ingratiate himself into their inner circle.

The actions demonstrated by PF09 allow comparison with three of Stotland's (1977, pp. 186-189) motivation classification types: 'sense of superiority', 'ego challenge' and 'power'. However, inconsistent with this classification system, there was little evidence of thrill-seeking behaviours or a heightened sense of his expertise. Instead, he was motivated by nothing more than the desire to be the centre of attention, where those he idolised would see him as an equal, something Goldstraw-White (2011, p. 85) referred to as an 'aspiring actor'.

The actions of PF09 were not limited to theft and disbursement of illegally obtained iPhones. Throughout his duties, he identified other criminals he had investigated, usually younger offenders; in these cases, he would advise them he had compiled an investigation and was ready to hand the file over to the local police authority. However, he would offer the criminal an alternative whereby they could pay the total value of their crime, in cash, directly to him. He falsely claimed he would return the cash to the organisation and the investigation would not be handed to police officials. So, on occasions, younger criminals paid the value of their crimes to PF09 and, true to his word, the investigations were closed. This modus operandi demonstrates that something other than Goldstraw-White's (2011) aspiring actor was at play—specifically greed and power (Ghazi-Tehrani & Pontell, 2021).

The transition from one motivational state to another was not unique to Case 09. In Case 10, the accounting fraud, the principal fraudster PF10 was initially motivated by the threat of loss of the service fees he was owed by his bankrupted client (Stotland, 1977, pp. 185-186). However, throughout the offending period, this too morphed into greed as he was promised commission fees on each new 'investor' he could introduce to the scheme. In this way, the insider case data show that motivations are not static, and instead evolve similarly to how other aspects of crimes evolve with time.

6.1.2.2 Suitable Victim

The insider data show that, in addition to each fraudster generally identifying different characteristics of what made a victim suitable, in a few instances fraudsters were influenced by multiple factors. The concept of target suitability represented different things to different offenders.[92] Traditionally target suitability, whether perceived or actual, included value, viability, ease of access and, at a more personal level, a chance to get even. In two of five cases,[93] familiarity influenced target selection because of the combination of both value and detailed knowledge of the financial systems and their internal controls (see Table 8). For example, in Case 04 involving theft by a union employee, principal fraudster PF04 operated in the organisation with complete authority, and through sheer force of will was never challenged by his colleagues or subordinates.

In Case 08, the fleet vehicle procurement fraud, the victim organisation had no oversight of procurement processes because of non-existent internal controls. Therefore, they could only rely on the word of principal fraudster PF08 who was an insider in their organisation. However, in the remaining three cases, access to the financial system was the central determinant of victim suitability.[94] Reasons for suitability in the cases varied but were in line with the justifications initially provided by Cohen and Felson (1979); however in two of five cases suitability was determined by several factors rather than one.[95]

6.1.2.3 Guardianship

The insider data found that, rather than an absence of capable guardianship, in most instances the guardianship in place did what it was designed to do. Cohen and Felson (1979) suggested that crime occurs in the absence of capable guardianship; however, the problem with this position is that it unhelpfully oversimplifies what are often complex situational

[92] ibid
[93] Case 04 / Case 08
[94] Case 09 / Case 10 / Case 13
[95] Case 04 / Case 10

factors. For example, in Case 08, the fleet vehicle procurement fraud, an absence of internal controls meant principal fraudster PF08 operated with complete autonomy in a multi-billion-dollar organisation, which exemplifies the absence of guardianship component of routine activity theory (Cohen & Felson, 1979). However, the data suggest that such instances are the exception rather than the rule. For example, the advent of password protection for computerised financial systems certainly satisfies the idea of virtual guardianship, until an offender gains access to passwords, as described by Detective N04:

> if you have the ability to access the system without leaving password trails or audit trails to say you are the person that entered, then yeah … it is very easy to commit a fraud, and also the access that [the principal fraudster] gained was he knew passwords of other people to enter [their] systems.

Overcoming guardianship via the unauthorised use of passwords is but one example of how capable system controls are breached. In Case 09, the theft by a telecommunications company employee case, principal fraudster PF09 instructed subordinates to teach him how their systems worked under the pretence that he needed this knowledge to complete his investigations. Likewise, in Case 13 involving insider trading fraud, seemingly complex and competent security systems designed to protect sensitive data were overcome in an incredibly low-tech manner. In this instance, the associate offender who worked for the organisation simply memorised what he read, walked out of his workplace at the end of his shift and supplied that information to the principal fraudster.

The data in Cases 04, 09 and 13 suggest that the guardianship provided by the internal controls arguably remained intact. Without the passwords of others, without someone explaining to a colleague how a particular system worked and without resorting to memorising data points, the inherent guardianship remained intact. This is because without resorting to these measures, other fraudsters would be unlikely to succeed.

6.1.3 Crime and Collaboration

The insider data suggest that collaboration was more common in insider cases than traditionally espoused. From Riemer (1941) to Avortri and Agbanyo (2020), and the decades and scholars between, the literature abounds with the idea of the solo fraudster, the insider who hides their crimes from others (Smith, 2014). Indeed, this is a central criticism of the models used to explain fraud, particularly the fraud triangle (Free, 2015; Morales et al., 2014).

Of the 13 cases outlined in Table 7, five were classified as insider cases. However, despite the prevalence in the literature of the archetypal solo fraudster, there was only one event that identified a fraudster operating independently from others.[96] In this instance, this was possible because the fraudster, an accountant, possessed the key components as described in the ALPi Model. Specifically, he had access to his clients' accounts, and extensive experience and knowledge of how to manipulate funds through seemingly legitimate business ventures; he planned his crime meticulously; and he was able to implement it without needing to involve others.

The principal fraudster in this case also closely resembled the fraudster described by Cressey (1950); that is, he had a non-sharable problem, was able to rationalise his behaviour and had the opportunity. In this case, the accountant had lost approximately AU$100,000 in service fees following the bankruptcy of a client. When presented with a seemingly legitimate investment opportunity to recoup his loss, he rationalised his unethical access and theft of clients' funds because the potential returns on the investment would recoup both his lost service fees, along with the monies he had borrowed from his clients.[97] As Detective N10 noted:

[96] Case 10

[97] Viewing one's actions as "borrowing" is what Sykes and Matza (1957) referred to as "denial of injury", and expresses the technique of neutralisation that attempts to view an action as immoral, but not criminal.

> he had access to the tax portals on behalf of his clients, so that was easy enough for him to manage. He had access to their actual accounts because they had given him access. On some occasions he was receiving mail from the banking institutions, he could change passwords without the client even knowing because all the correspondence was always sent to him as the accountant, so his access was pretty good.

Contrasting with this were the four remaining insider cases in which the principal fraudsters colluded with others. In one of those, Case 09, the principal fraudster PF09 collaborated with his co-worker AF09. While AF09 provided no additional access, knowledge or skill to the enterprise, his involvement lessened the chances of detection by others. AF09 was the line manager of PF09 and played the role of protecting PF09 from discovery by covering up facts on occasions when PF09's activities were questioned.

In Case 13, the insider trading fraud, the principal fraudster PF13 required the support of an outsider who had access to and knowledge of sensitive government data. This allowed PF13 to gain an unfair advantage over other entities undertaking what is commonly referred to as 'news trading'. In this case, the absence of AF13 would have made this crime impossible, and thus collusion was critical to the success of the principal fraudster's scheme.

A final grouping identified from the insider case data included two cases.[98] In these cases, the collaboration involved a combination of both insiders and outsiders. In Case 04, theft by a union employee was evidenced on two occasions. The first was through the provision of supplementary credit cards by AF04c and AF04d to PF04 so he could spend on his election campaign with a trade union without the victim organisation's knowledge. In this instance, PF04 paid AF04c and AF04d back for his use of the credit card using corporate cheques from the victim organisations, and authorised those payments in a way that restricted

[98] Case 04 / Case 08

oversight. On the second occasion, PF04, as already discussed, engaged a corporate supplier (AF04e) to over-invoice the victim organisation, with the surplus monies split between PF04, AF04a and AF04e. The way that access to the financial systems was achieved in this instance was first via AF04a, the procurement manager of the victim organisation; and second, via the owners of several external businesses that supplied products and services to his organisation. In combination, the three components of this syndicate—the union general secretary, procurement manager and external suppliers—were able to provide access to all necessary financial systems. This resulted in overbilling with profits being split across the syndicate.

The form of collusion that occurred differed across four of the five insider cases. In three of those four cases, the collusive relationship arose within the workplace,[99] with the fourth arising in a social setting.[100] An alternative approach to classifying identifiable differences between collusive groups was proposed by Free (2015). For instance, in Case 13 collusion was the result of affective bonds, characterised by connection via kinship or friendship. In Case 08, the fleet vehicle procurement fraud, collusion was revealed as a by-product of organisation-serving functional bonds, whereas Cases 04 and 09 represented individual-serving functional bonds, in that by collaborating the wider group stood to gain more. Ultimately, among the cases presented in this section, collusion was confirmed in four out of five instances because the principal fraudster lacked, to some degree, the necessary level of access, knowledge or skills[101].

6.1.4 Conning Their Way in

Unsurprisingly, the insider data reveal the deployment of personal resources in the fulfilment of crime (Ekblom & Tilley, 2000). To understand how access occurs in insider crimes, consideration should be given to personal power and personality characteristics, since

[99] Case 04 / Case 08 / Case 09
[100] Case 13
[101] While multipule fraudsters were observed in four of five cases, in Case 09, AF09 did nothing more than protect PF09 from internal oversight.

status, privilege, and power derived from elite or executive occupational roles has a significant influence in determining the likelihood of reporting, detection and even prosecution (Pontell, 2016). For example, in the absence of legitimate access to systems like accounts payable or stock management systems, a competent fraudster will deploy personal resources including persuasion or force of will (Ekblom & Tilley, 2000). As was observed in Case 04, PF04 did not have legitimate access to accounts payable, but what he did have was a position of authority as the head of the organisation, coupled with a level of financial delegation authority that did not extend to accounts payable. The normal process involved relevant staff and suppliers raising payment orders that would be checked and authenticated by the financial controller, OT04a. These were then approved by PF04 in his position as union general secretary. However, what PF04 did instead relied on the fact that the board had provided him with financial delegation powers and authority to use in the best interests of the organisation. He prepared fraudulent payment orders, signed them off and handed them to OT04a for processing and payment. Despite this seemingly obvious irregularity, PF04, through sheer force of character, intimidated his staff into complying, as one staff member remarked: 'he was very busy and was quite an intimidating person, and I developed a perception that he was a very powerful figure both in the [organisation] and outside'.[102] Another staff member stated:

> Although [he] did not threaten [the suppliers] with losing their contract, I felt that in the context of the meeting it could easily be interpreted that's what could occur or may result if they did not do what he asked … [he] had a very aggressive personality and asserts his control in meetings when he wants people to agree with him or go along with what he wants them to do.[103]

[102] Case 04 Statement OT04b
[103] Case 04 Statement AF04a

This shows that despite the presence of controls that inhibited the plans of PF04, he intimidated and bullied staff and external contractors who provided him access to the financial systems. Therefore, despite a lack of legitimate access, an autocratic personality used in the right circumstances ensured important aspects of the frauds moved ahead as planned. This is evidence that when legitimate access is blocked it can be achieved through fear and intimidation.

In direct contrast to the fear-driven approach seen in Case 04 was the charming and charismatic, yet equally effective personality deployed by the principal fraudster PF09 in Case 09 involving theft by a telecommunications company employee. In this instance, PF09, a former fraud squad detective, relied on personal resources to achieve access to systems (Ekblom & Tilley, 2000). He used his authority, coupled with a charming personality, to garner access to systems. For example, Detective N09 observed:

> He took advantage, he got access to some of the systems, even by sweet-talking people, you know, 'Oh Sheryl, toots, what I really need for this investigation is access to this ordering system' and she would say 'you're supposed to go to Helpdesk,' and he goes 'just this once', so he would use his charisma.

In both instances described in this section, the relevant internal controls were in place. However, the two principal fraudsters applied different personal resources to achieve their aim of defrauding their organisations (Ekblom & Tilley, 2000).

6.2 Access and the Outsider

In comparison to the malicious insider, less is known about fraudsters as outsiders, and how they access their victims. What can be drawn on is often linked to other forms of financially motivated crime such as burglary (Felson, Jiang, & Xu, 2020; Meenaghan et al., 2020) and robbery (Bourgeois & Fisher, 2018; Hipp, Kim, & Wo, 2020). One reason for the limited focus on fraudsters as outsiders is that these other financially motivated crimes are

almost solely committed by outsiders (Riess, 2011), whereas frauds are more commonly associated with insiders.

In the absence of a developed body of literature on how fraudsters, as outsiders, gain access to their targets, it is possible to begin with a series of assumptions based on what is missing from the mainstream literature. For example, studies that have analysed the behaviours of insiders often identify collusion with external criminals (Australian Government, 2016; Carnegie Mellon University, 2012). This identifies the potential for pre-employment and post-employment subversion of insiders, as is commonly discussed in the IT security literature (Walton, 2006). From there it is possible to propose that where insiders are being subverted, either pre-employment or post-employment, outsiders are deliberately taking steps to achieve this outcome.

Other avenues open to examination from an outsider's perspective are the numerous studies exploring specific frauds that concentrate on organisational interface points including call centres (Selzer, 2006), mortgage applications (Herndon, 2019) and procurement systems (Doig & Sproat, 2020). Most of these studies have focussed on the crimes, controls and characteristics of the offenders; few have concentrated on the outsider status of the fraudster. Ultimately, such omissions undermine efforts to fully understand how proximity to financial systems influences the implementation of tradecraft by fraudsters, which is drawn out in Table 9.

Table 9

Outsider Case Access Characteristics

	Mode of access						Subversion of insider		Motivation*			Victim suitability							Guardianship								Organisational interface				
																Absence of guardianship			Regulation-driven internal policies											
Case	Routine daily activities	Specialised access positions	Paid-for access	Hacking/skimming	Sales and billing	Finance application forms	Pre-employment subversion	Post-employment subversion	Primary	Secondary	Tertiary	Familiarity	Social connections	Trending crime	Organisational interface	Weak controls	Weak penalties	Anonymity	Multi-factored verification	Internal & external audits	Financial delegation	Whistleblowing	Customer due diligence	Organisational culture	Anti-tampering	Shifting responsibility	Consumer banking	Consumer finance & mortgage applications	Debt-factoring	Point of sales	Procurement
01	X	X			X			X	TL	M	EC	X			X	X				X	X	X		X						X
02			X	X					M	A				X		X			X				X			X	X				
03			X			X			M				X		X				X	X			X					X			
05		X		X				X	M	A				X		X	X	X	X	X					X	X			X		
06		X	X	X			X	X	M	B				X		X	X	X	X						X				X		
07	X	X			X	X		X	TL	M	B	X			X	X				X											
11	X	X				X		X	M			X			X	X			X	X			X					X			
12	X	X						X	M			X		X						X					X						

Note. * TL, threat of loss; M, money; A, addiction; EC, ego challenge; B, benefactor

X – indicates a positive correlation between the χ-axis and the γ-axis

6.2.1 It's Part of 'Their Job'

Whereas the insider case data linked Cohen and Felson's (1979) work on routine activities to principal fraudsters' occupational positions, the outsider cases linked it to associate fraudsters' occupational positions. Therefore, while this signified that routine activities and, through it routine activity theory, was again able to account for access via employment, it was the 'who' that changed. This signified that in the absence of personal access, principal fraudsters gained access via others occupational positions.

As identified in Table 9, four of the outsider cases identified that some degree of access was drawn from routine daily activities.[104] What differs here is that the cases depicted in Table 9 are those where the principal fraudster was an outsider to the victim organisation, rather than an insider. Nonetheless, it was evident from the case management files that routine daily activities still played a role. The difference, however, in this classification is that those who acquired the necessary access, knowledge and skills were not the principal fraudsters; instead, they were criminal associates operating under direction from a principal fraudster, an issue addressed later in this section 6.2.4.

In each of the four cases, the associate fraudsters as insiders possessed the necessary access, knowledge and skills for the successful execution of their fraud.[105] This indicates that in these investigations it mattered not whether the principal fraudster was an insider. Instead, as long as one member of a criminal syndicate had access via their employment, routine activity theory is still an applicable explanation because motivated offenders (associated offenders) encountered a suitable victim in the absence of capable guardians (Cohen & Felson, 1979).

[104] Case 01 / Case 07 / Case 11 / Case 12
[105] ibid

6.2.1.1 Motivated Offender

In the outsider cases, the first aspect of Cohen and Felson's (1979) hypothesis, the motivated offender was evident; and again, as seen in the insider data, this varied (see Table 9). The outsider selection of cases shows that greed was the primary motivator (Stotland, 1977),[106] with the threat of loss the only other primary motivating factor[107] [108]. There was, however, great diversity in regard to the presence of secondary motivations in five of the cases, and tertiary motivations in a further two[109] [110]. Viewing motivation in this way, as primary, secondary and tertiary motivations, provides an account of the evolution of motivation over time as situational factors changed. For example, in Case 07, the debt-factoring fraud, the principal fraudster PF07—the proprietor of a vehicle service company facing financial difficulties—initially committed her frauds to stave off the collapse of her business with the intent of repaying the stolen money, akin to Stotland's (1977) threat of loss classification. However, over time her motivation evolved, and greed became more readily apparent (Stotland, 1977). Finally, PF07 appeared to be drawn on by the personal fulfilment she gained from her generosity to the community. In a way this was a form of criminal altruism, described by Detective N07 as:

> she likes to play the part of the benefactor; she loves that feeling where she can give gifts to people. 'Oh, look she just gave us fifteen hundred dollars' worth of sponsorship for our underage soccer team'. She loves everyone looking at her thinking she's a hero.

In other cases, an unexpected motivation arose at the secondary stage.[111] As outlined in Table 9, Cases 02 and 05 involved both gambling, and drug and alcohol addiction as

[106] Case 02 / Case 03 / Case 05 / Case 06 / Case 11 / Case 12
[107] A classification put forward by Stotland (1977)
[108] Case 01 / Case 07
[109] Case 01 / Case 02 / Case 05 / Case 06 / Case 07
[110] Case 01 / Case 07
[111] Case 02 / Case 05

secondary motivational factors driving separate criminal syndicates (Sakurai & Smith, 2003). As Detective N07 noted:

> A lot of the guys have some issues with drug dependence. They are greedy; they find ways to make money without working for it properly and so none of them have jobs. They spend their time trying to steal money and doing drugs.

Motivation, as expressed in the outsider cases, is unsurprisingly dominated by money or greed in explaining why these crimes occurred, with 8 of 15 explanations attributed to this reasoning. However, the presence of a threat of loss,[112] addiction[113] and ego challenge demonstrated the diversity of motivations, which supports the premise that motivation is not a static phenomenon; rather it evolves in line with changes in personal and situational factors.[114] The analysis also identified the absence of two of Stotland's (1977, p. 188) concepts of power: 'the satisfaction [of] holding down positions of great power in some organisation'; and group forces which were described as:

> situations in which fraud occurs as a part of a business but is not the main purpose of the business. In the General Electric case, many of the actual perpetrators of the violations of the antitrust laws were fully aware of the criminal nature of what they were doing. But they perceived that their superiors in the company expected them to participate (Stotland, 1977, p. 190).

6.2.1.2 Suitable Victim

The data suggest the presence of a greater variety of factors influencing victim suitability in the outsider cases than was observed in the insider cases. The outsider data, set out in Table 9, differed from the insider data, set out in Table 8 in respsect to why victims, individuals or organisations were deemed suitable by the offenders. In all cases, more than

[112] Case 01 / Case 07
[113] Case 02 / Case 05
[114] Case 01

one criterion was identified. For example, the analysis of Case 01 identified familiarity with the system, legitimate pathways to the financial systems and weak internal controls as primary reasons for victimisation.

In this case, the two associate offenders—the executive general manager of IT operations (AF01a) and the general manager of IT infrastructure (AF01b)—were familiar with the organisation's procurement processes as these fell within their operational remits. Next, they identified an opportunity to abuse trust placed in them by their employers by using existing procurement processes, coupled with their delegated financial authority.[115] Finally, the two associate offenders were familiar with the organisation's internal control processes as they were both responsible for the maintenance of internal risk registers. This enabled them to identify and capitalise on existing weak internal control processes.

Weak internal controls were the most cited influencer in regard to the suitability of a victim.[116] This highlights the possibility of a level of rationality in the decisions made by the principal fraudsters in those cases. This is not to say other crimes were irrational; rather that, in the six cases identified, the weakness of internal controls provided the opportunity to exploit the victim. Perceptions of control inefficiencies were also common across the cases with examples of irregular audits,[117] failing to conduct basic customer due diligence checks[118] and failing to check the checkers, as described by Detective N01:

> Controls keep honest people honest; controls do not stop dishonesty. If someone goes in with the intention of committing a dishonest act they will simply go round the controls, the control is like a road barrier, 'there is a road barrier there you can't cross it', yes you can you just step over the top of it. 'Well, that's against the law', well that

[115] (Cressey, 1950)
[116] Case 01 / Case 02 / Case 05 / Case 06 / Case 07 / Case 11
[117] Case 05
[118] Case 02

only bothers people who are bothered about the law. So, if you are going out to break the law the barrier is of no interest to you, it is just something to work around.

Another commonly cited reason for victim suitability was the presence of organisational interfaces.[119] An organisational interface describes how an organisation's financial system facilitates a legitimate connection between the fraudster and the target financial system. This may involve mortgage and credit application processes,[120] and procurement processes and accounts receivable operating between different businesses.[121]

Trending crimes were also popular among technically efficient and generally younger criminals.[122] Trending crimes describe what might otherwise be known as a wave of similar crimes. At the time of data collection, card skimming crimes were popular, with numerous media reports of offending across Australia (Brown, 2015; van den Broeke, 2015; Wuth, 2015). Examples of this are the card skimming and account takeover crimes in Cases 02, 05 and 06, which targeted credit and dedit card weaknesses and were but three of dozens of investigations underway in the relevant jurisdictions at that time. Analysis of other cases revealed a modus operandi imported from overseas, meaning the frauds had been operating successfully overseas and had been imported by criminal syndicates into the Australian criminal marketplace.[123] Australia's relative unawareness of these newer crime types, as they were at the time, in part increased their attractiveness to criminal syndicates. As noted by Detective N06:

because they'd utilised this crime type over in England and other countries effectively, they slipped in under the radar … if you get away with it in England or

[119] Case 01 / Case 03 / Case 07 / Case 11
[120] Case 03 / Case 11
[121] Case 01 / Case 07
[122] Case 02 / Case 05 / Case 06
[123] Case 06 / Case 12

> Canada or America, you come to Australia where you think the land down under, she'll be right mate, you think you'll get away with anything.

Cohen and Felson (1979, p. 591) contended that target suitability would reflect 'value (i.e., the material or symbolic desirability of personal or property target for offenders), physical viability, access, and the inertia of a target against illegal treatment by offenders'. However, it was evident in the outsider case data that a broader range of factors contributed to the perceived suitability of victims, including the risk of detection and obfuscation of offender actions.

6.2.1.3 Guardianship

The outsider case data, much like the insider case data, offer a diverse array of controls both in terms of their breadth across an organisation and in the marked differences in how many, or how few were deployed across different organisational settings.

As Table 9 shows, an array of guardianship measures were in place across the organisations and in each instance these controls failed to some degree. However, as identified in the insider case data, suggestions of no capability or an absence of guardianship oversimplifies what are complex situational factors. For example, in Case 01, the victim organisation had an array of internal policies all aimed at preventing procurement fraud. For instance, AF01a and AF01b had financial delegation authority capped at AU$1 million, which necessitated action on the part of the fraudsters. As noted by Detective N01:

> In a series of emails around 24 January 2014 staff at [PF01's company] discuss the fact that they are overcharging for some aspects to such a degree that they are concerned it would draw attention to aspects of the deal. In a reply from [one of PF01's employees who knew the fraudulent nature of the deal], he states, 'The status is that [AF01a] and [AF01b] are willing to sign off a total of value of $AU6.9 Million

(US$6.5 Million) in TDs [Transaction documents].[124] However, we need to keep each TD [transaction document] under $1Million in licenses for him to be able to do this. Is there a way we can break down TD 17, TD 22 and TD 23 so we end up with six TDs instead of three for these pieces?'

Next, internal audits performed by staff under the control of AF01a picked up these financial irregularities but did not link them to the offenders. The whistle blower, who unknowingly brought these findings to the attention of the associate offenders, was promptly made redundant. They simply responded to this threat by restructuring his role under the auspices of cost-saving measures. Finally, the associate offenders were responsible, within their respective areas, for the maintenance of effective corporate culture and were known to dismiss subordinates for much less serious breaches; yet they perpetrated an AU$14 million fraud. As such, in every sense the controls in place were capable, in so far as they picked up on the inappropriate behaviours they were designed to weed out, but on every occasion, they were set aside by the people they were intended to identify.

6.2.2 Organisational Interface Points

An absence of alternative access means some fraudsters will seek to access a financial system via interface points. An interface describes an aspect of an organisation's business model that facilitates interaction between the organisation and those entities with which it interacts. For example, a customer interface could be a mortgage application form, while an example of a contractual interface might be a procurement process interaction between the organisation and its suppliers. These interfaces points provide criminals with opportunities to interact directly with exploitable aspects of an organisation.

Cases 03 and 11 were investigations into criminal syndicates that targeted consumer finance and mortgage application interfaces at two major Australian financial institutions. In

[124] Transaction documents include all documents relating to the purchase of goods or services.

Case 03, the mortgage and finance fraud case, syndicate members would steal the identities of victims and use them to obtain finance for a range of items including high-end motorcycles and luxury vehicles. These would then be used or sold on while the finance loans defaulted through non-payment. In one example, the principal stole the identity and funds from a terminally ill woman when preparing to finance the purchase of three Harley Davidson motorcycles, which the fraudsters intended to use to run a Harley Davidson tour company. This plot was not well regarded by associate fraudster AF03a, who noted, 'What sort of thieving low cunt robs money that a dying chick with cancer was using to take her kids to Disneyland?'.

In Case 11, the land valuation mortgage fraud, syndicate members acquired cheap western NSW residential bocks of land for as little as AU$5,000 each. Then, through a series of fraudulent paper-only transactions, they inflated the price of the properties until each reached approximately AU$250,000. The syndicate then used the mortgage application process of a large Australian financial institution to take out loans using the fraudulently valued properties as collateral. This crime was backstopped by a post-employment subverted insider. The principal difference between these two crimes was that in Case 03, the mortgage and finance fraud case, the fraudsters relied on the strength of their application using the stolen identities of others, whereas Case 11 relied on fraudulent valuations and an insider to ensure the crime was executed as intended. This difference provides another example of subtle differences between broadly similar crimes.

Fraudsters in the outsider cases also relied on a debt factoring interface. In the automotive services sector, some companies on-sell their debts to other businesses specialising in debt factoring. Debt factoring allows a company (A) that is owed money by another company (B) to sell company B's debt to a debt factoring business (C), minus a commission. This allows company A to continue trading while company C takes the

responsibility for collecting the debt from company B. Through her ownership of an automotive services company, principal fraudster PF07, in Case 07, used existing relationships with debt factoring companies. Using their debt factoring services, she submitted an initial debt factoring request to one debt factoring company when there was no debt owning. When the first debt factoring company was due to be paid, the principal fraudster then factored another fraudulent debt from a second company to pay the first. Each time the principal factored another debt the cost of that debt increased to cover the debt factoring company's commissions and to furnish the extravagant lifestyle of the principal fraudster. Eventually, over time this crime become increasingly unwieldy, as Detective N07 remarked, 'so effectively what she's done, is she's created a Ponzi scheme, and she's self-ponzied'.

Similarly, Case 01 relied on a procurement systems interface. In this instance, the principal fraudster PF01 was the CEO of an IT service provider that was in the process of being sold by PF01 to another IT company. The sales agreement provided a flat payment of just over AU$160 million. However, there was an enticer thrown in by the purchasing company: should the principal fraudster's company make an additional AU$98 million in sales over a defined period, the principal fraudster would receive an additional AU$30 million. As the principal fraudster was approximately AU$14 million short of that target, as outlined in Case 01, through a process of bribery and corruption he subverted two insiders in the victim organisation. With the assistance of the two subverted insiders, PF01 then identified and used the victim's procurement interface to meet the shortfall in his company's sales. As described by Detective N01, AF01a and AF01b facilitated this by purchasing software from the principal fraudster's company, that the victim organisation did not need: 'if you look at what these guys did, which resulted in a hundred-million-dollar fraud and two

and a half million dollars' worth of kickbacks using 14 million bucks' worth of [the victims] money, they brought software they never needed'.

Other examples of commercial interfaces include consumer banking interfaces such as those in account takeover frauds like Case 02. Following the theft of a customer's identity, which occurred because of a hack or purchase of stolen details online, the fraudsters used stolen identity details to withdraw funds in person from a victim's bank accounts. In this case, the commercial interface was provided by the victim's bank, which provided over-the-counter withdrawal services for customers.

In Cases 05 and 06, the commercial interfaces that were exploited were point of pale devices (POS). These devices, used by retailers, were fraudulently converted to capture Track 1, Track 2 and PIN data from unsuspecting consumers who visited service stations around Australia. The stolen data were used to create cloned debit cards, which were then used to withdraw funds from victims' accounts at ATMs. In Case 05, the card skimming of taxi patrons, access was achieved via the post-employment subversion of taxi drivers who provided the criminal syndicates with access to their vehicles, where skimming devices were installed and downloaded in exchange for a fee.

Access in Case 06, the card skimming at service stations, again via compromised POS devices, used several methodologies. Initially, the syndicate inserted compromised terminals without the merchant's knowledge; they then progressed to subverting individual employees. As noted by Detective N06, the syndicate then began to pay off merchants for access:

> they even went to the extent of buying a service station up in Forster, and we monitored it and observed … well they leased it and then did badness and then reneged on it and yeah legged it. Yeah, up, and left, just drove out, see you, [customers were] standing at the bowsers saying, 'what the fuck!'.

6.2.3 Secondary Systems Access

The presence of organisational controls, themselves designed to protect a target financial system from abuse, often pushes a criminal to compromise a secondary system to overcome the controls in the target financial system. For example, in Case 02, before the account takeovers via call centre pathways could occur, the principal fraudster needed to build up identity bundles.[125] To do this, he purchased stolen identities and bank account details from dark websites known as carding portals.[126] As described by Detective N02, these stolen identity bundles were then added to by the syndicate:

> The boss then checks the data to determine whether there is a potential victim with money in their account. Then once they have checked the account, they will build a profile on that victim, obtaining more identification information about that individual. When they are happy with the amount of identification they have, they begin creating false documents, such as drivers' licenses, and all the other bits and pieces they normally do, telephone bills, Medicare cards, things like that, and then they make a 100-point ID bundle.

In other instances, the principal fraudsters sought to themselves access other systems directly in their efforts to build identity bundles. As noted by Detective N02, 'they hacked into a financial planner's computer; they got all the data from the financial planner on his customers. They also hacked into a payroll company'.

In the two previous examples, the principal fraudsters accessed other systems to collate data before the substantive crime that targeted financial institutions could occur. These cases of secondary

[125] See Methods Chapter Footnote 41

[126] Detective N02 'In relation to the actual commission of the offence there is a lot of preparation involved, in Case 02 they were getting information from Hackers which we believe were overseas in the form of BotNet Logs. A BotNet is basically where a normal standard computer is called a Bot, that machine gets infected, there's a few ways they can do it, say a phishing email where they draw you to a site, basically your machine is infected, they've got the Bot, it gets infected basically hangs around and does stuff like record your key strokes and when that happens and it detects a user name and password for a bank account it gets fed to the control server which is usually overseas, mostly in China and Russia most of them are'.

access highlight that, rather than just accessing a victim's financial system, fraudsters often commit other crimes to satisfy their information needs before the substantiative crime. Regardless of whether this access was gained via paid-for dark web carding portals as in two cases;[127] the by-product of hacking attacks as the case in three crimes;[128] or through legal channels such as property ownership checks, the result was that secondary access incursions provided the information the fraudsters needed to overcome controls.

6.2.4 Subverting Insiders

The outsider data suggest subversion was, in nearly all instances, critical to the success of the fraud. If access to target financial systems or even secondary systems is difficult, outsider fraudsters often resort to the subversion of insiders. This was a prominent pathway available to the outsiders in the cases seeking to compromise the integrity of a target financial system. Six of eight cases involved post-employment subversion,[129] and one of those also involved pre-employment subversion (see Table 9).[130] The desirability of turning insiders to the principal fraudster's cause is obvious. Insiders offer established access and are less likely than outsiders to be subjected to additional levels of scrutiny; therefore they are a logical choice for the principal fraudster.

Subverted insiders also provide invaluable knowledge of the workings of the targeted financial system; however, there is debate as to the level of loyalty they may offer the outsider. Walton (2006), for instance, suggested that greater levels of loyalty towards principal fraudsters would be evident in pre-employment subversion than in post-employment subversion settings, as insiders subverted before employment are more likely to know their involvement is criminal. Therefore, they are logically less likely to tip off their employers, whereas a post-employment subversion must overcome years of familiarity and loyalty to the

[127] Case 02 / Case 03
[128] Case 03 / Case 05 / Case 06
[129] Case 01 / Case 05 / Case 06 / Case 07 / Case 11 / Case 12
[130] Case 06

organisation and colleagues, which presents a greater degree of risk. Loyalty aside, another factor making pre-employment potentially riskier is the potential for violence directed towards non-compliant syndicate members. As described by Detective N06 when a criminal syndicate turned on one of their pre-employment subverted insiders:

> the student got cold feet, and they started threatening to kill him. This is how serious they get; stabbing, shooting, they beat him up. All these things they got up to, the day of the arrests, they were out actively hunting him down.

Case 06, the card skimming at service stations case, points to instances of both pre- and post-employment subversion. In that investigation, the criminal syndicate aimed to capture EFTPOS Track 1 and Track 2 card data, along with users' PINs. Armed with these data, the offenders coded the stolen Track 1 and Track 2 card data onto blank EFTPOS cards. Runners (lower-level syndicate members) used the cloned cards to withdraw as much money as possible from victims' accounts before detection.[131] This was achieved by withdrawing the daily cash withdrawal limit immediately before and after midnight. This strategy was advantageous because it limited the exposure of the syndicate's runners to risk of detection as they used the cards only twice in the space of an hour before disposing of them. Further, it allowed syndicate members to access victims' bank accounts by working around financial institution controls, where daily limits restricted the amount of funds that could be withdrawn from accounts via ATMs. As noted by Detective N06:

> here's 20 or 50 cards, go and withdraw daily limits on all these accounts, they are blank cards, so normally white or silver or gold or red, depending on the manufacturer's colour, no marking on them other than a magnetic strip on the back, and then quite often a paper sticky dot with the four-digit number being the pin, and

[131] A "Runner" is another term used to describe low-level members of a criminal syndicate. It is often used interchangeably with the term "mules".

> they go out and they will stand at an ATM and just run the cards through withdrawing the daily limit. If they are smart they will do it late at night, wait till the next 12 o'clock kick over so they can get the next lot of money; two lots in one hit.

Pre-employment subversion was observed on several occasions across the investigation. As noted by Detective N06, the first involved gaining access to resources:

> They infiltrated the manufacturers of the POS, or aspects of the POS.[132] They infiltrated card manufacturers, the PVC plastic cards and magnetic cards, so they have free access to blank cards they then infiltrate the manufactures of the devices, the most recent technology, where they are upgrading software, or changing software in terminals.

This example of pre-employment subversion provided the syndicate with access to the resources and technologies they needed to implement their crimes directly from the overseas manufacturers. These were shipped to Australia where they were modified by the syndicate's technicians to capture Track 1 and Track 2 data of unsuspecting members of the public who used their debit and credit cards in businesses where these fraudulent devices had been installed. As described by Detective N06, another example of post-employment subversion then occurred; this time the syndicate identified suitable merchant locations:

> pressuring them, promising them money, paid some funds, met in person at a public location, where they couldn't be monitored, then installed the POS device. It was offline so they arranged for payments to the merchant because he obviously had to make it look like he was still trading.

Post-employment subversion in this instance provided the syndicate with access to a merchant's clientele, whose debit and credit card data would be captured by the compromised

[132] POS is a shorthand term used by detectives to describe Point of Sale devices in businesses that take debit and credit card payment. POS does not include automatic teller machines (ATM's).

POS devices. However, to facilitate this without drawing undue attention to the merchant, the syndicate then entered another period of pre-employment subversion. As noted by Detective N06:

> they then obtained a fraudulent driver's licence, fake identity for a student—we'll call him Harry—who had to be an employee in the shop because they wanted to establish plausible deniability for the merchant, and there is CCTV in the shop and they wanted 'Harry' to come in with his fake driver's licence and apply for a position in the shop, which he would be given; he would then swap out the terminals.

This alternating process of post- and pre-employment subversion provided the syndicate in Case 06 with resources that, when combined, both provided access to a merchant location and enabled the installation of the compromised POS devices in a way that would distance the merchant from the criminal syndicate.

Post-employment subversion was also seen in several other cases.[133] Case 12, the superannuation fraud, provided an interesting example of post-employment subversion where two insiders—one in the victim organisation and a second in a telecommunications company—were subverted by the principal fraudster PF12a, which resulted in a successful fraud netting the syndicate AU$150 million. The roles these two insiders played were different. The telecommunications insider AF12b facilitated access to a telecommunications exchange and identified a secure line between the victim organisation and one of its trading partners. This enabled AF12a to send a fraudulent funds transfer request and respond to the victim organisation's security phone call-back, used to confirm the validity of transactions. The second insider, AF12c, in the victim organisation supplied the syndicate with information about how funds transfer requests were submitted, validated and approved, and guided the fraudulent funds transfer request on the day of the crime. As identified in the

[133] Case 01 / Case 05 / Case 07 / Case 11 / Case 12

outsider case data, the role of pre- and post-employment subversion has an impact on the success of criminal events. As is shown by the fact that these crimes were successful, subversion provided principal fraudsters with the ability to avoid or overcome most internal controls that organisations put into place.

6.3 Summary

Unsurprisingly, the analysis supported the premise that principal fraudsters, as insiders, gained access to their target financial systems via employment, highlighting the fact they were likely to have an easier task of exploiting system vulnerabilities than were outsiders. Lacking this obvious advantage, outsiders needed to perform a greater number of activities to gain the same level of access. Logically then, insiders are likely to display lower activity levels earlier along their fraud event timelines than are outsiders. However, despite occupational positions, access did not occur automatically for all insiders, all the time. This was due in part to 1) the need to overcome the SOD barriers within organisational settings, and 2) the fact that not all insiders had the authority to access all the internal systems they needed to operationalise their crimes. This necessitated a blend of opportunistic and planned activities to secure access to all internal systems. Outsiders also relied on a blend of planned and opportunistic activities to access the internal systems they needed to. In the only case where opportunity was flagged as an enabling factor, the principal fraudster—having worked closely with the victim organisation over many years—relied on this business connection to gain access.[134] In the remaining outsider cases, access was the outcome of deliberately planned actions.

[134] Case 07

In both the insider and outsider cases, greed was the dominant motivating factor,[135] followed by a threat of loss[136] and ego challenge (Stotland, 1977).[137] Most of the insider cases demonstrated a transition to secondary motives including a sense of security, the threat of loss and greed (Stotland, 1977). Outsiders also demonstrated greed,[138] addiction,[139] benefactor[140] and ego challenge as secondary and tertiary motivations.[141] The presence of these second and third-order motivations reveals that greed and the threat of loss, the two most common initial motivating factors, were in most instances quickly augmented by other motivations.

Victim suitability from the perspective of the insider was deemed to be largely derived from positions of employment. However, the outsider data reveal that rather than a single factor influencing target suitability, the cases demonstrated multipule factors per case. The most cited factors that influenced target selection were weak internal controls,[142] followed by familiarity,[143] trending crimes,[144] and the presence of accessible and exploitable commercial interface points.[145] Suitability, informed by familiarity, was representative of cases where insider associates were involved in the upfront planning and decision making; whereas cases with insider associates not involved identified other factors as influencing target selection. This is likely because of the confidence the insiders brought to the principal fraudsters' decision-making processes. Another key factor driving target selection was the apparent newness of card skimming crimes across Australian jurisdictions.

[135] Case 02 / Case 03 / Case 04 / Case 05 / Case 06 / Case 08 / Case 11 / Case 12 / Case 13
[136] Case 01 / Case 07 / Case 10
[137] Case 09
[138] ibid
[139] Case 02 / Case 05
[140] Case 06 / Case 07
[141] Case 01
[142] Case 01 / Case 02 / Case 05 / Case 06 / Case 07 / Case 11
[143] Case 01 / Case 07 / Case 11 / Case 12
[144] Case 02 / Case 05 / Case 06 / Case 12
[145] Case 01 / Case 03 / Case 07 / Case 11

Trending crimes linked to the affordances of new technologies became apparent around 2010 to 2011, when compromised POS technologies began to enter the Australian criminal marketplace.[146] The nature of these devices pointed to the necessity for fraudsters to place them in locations with high card traffic and low oversight. This suggested it was not a victim's suitability that influenced their victimisation; rather that they simply frequented a particular business location chosen by the criminal syndicate. This indicates that victim selection is not always deliberate, but may be a by-product of other situational factors. The data also revealed that in seven of eight outsider cases the principal fraudsters used commercial interface points to access their victims.[147] The interface points included financial and mortgage application products, customer service facilities, accounts receivable systems and POS systems. The data identified that these systems were targeted because they were readily available, high-volume systems with a potential for a high rate of return on the schemes devised by the fraudsters. However, since these systems are known hotspots for frauds, several existing control measures needed to be overcome to gain access. To overcome controls such as identity verification processes, the fraudsters required access to several secondary data sources including companies' staffing records, which assisted in the construction of 100-point identity bundles. Therefore, secondary access via predicate offences, in almost all cases provided syndicates with the necessary information to execute their frauds against their intended victim systems.

Guardianship, on the face of it, failed in each case. Nonetheless, the data suggest that controls were in place in each organisation and worked as they were designed to, with the obvious exception of Case 08, where there were no internal controls. This counterintuitive statement is explained by the fact that in nearly all cases, the internal controls forced the

[146] Case 02 / Case 05 / Case 06
[147] Case 01 / Case 02 / Case 03 / Case 05 / Case 06 / Case 07 / Case 11

fraudsters to devise ways around them, which in nearly all cases led to the detection of the fraudsters. Rather than viewing guardianship as incapable, this points to an increased level of capability of the fraudster, without which another, less skilled fraudster, is unlikely to be successful.

The insider data show that in four of five cases, collusion was evident with differing combinations including principal/insider, principal/outsider and principal/insider/outsider. [148] Thus, collusion was found to augment the principal fraudster's lack of access, knowledge or skills, and was a deliberate choice guided by the principal fraudster's awareness of their information and access deficiencies. This indicates that despite the common perception of the lone fraudster (Cressey, 1950; Free, 2015; Riemer, 1941), offending alone is only possible where the fraudster can implement every stage of their crime without the support of others' access, knowledge or skills. Outsiders, in contrast, turned to subversion to overcome their access limitations in six of eight cases.[149] In those six cases the insiders, regardless of whether or not they were involved in the upfront planning and decision making, facilitated access on behalf of the principal fraudsters.

[148] Case 04 / Case 08 / Case 09 / Case 13
[149] Case 01 / Case 05 / Case 06 / Case 07 / Case 11 / Case 12

Chapter 7: Tradecraft—Learning in Financial Crimes

Knowledge is crucial to complex frauds. The application of deceptive strategies designed to convince entities to divest possession of something of value is central to successful frauds. However, as an organisation's financial resources are generally protected by control mechanisms, it is unusual for fraudsters to simply take funds physically. Therefore, to achieve this aim, successful fraudsters devise methods of bypassing controls. To do this, they require a working knowledge of how the target financial system operates under normal circumstances. Additionally, they must understand the nature of the controls and how, when triggered, the controls respond to breaches. Thus, principal fraudsters require a degree of knowledge about the financial system and its controls to allow them to steal funds from the victim while remaining undetected.

This chapter explores variation in the acquisition of criminogenic knowledge across the insider and outsider cases. The second of three chapters aligned to the ALPi Model, this chapter acknowledges that learning occurs in more ways than one. As was the case in Chapter 6, the central determinant of variation among most cases was the proximity of the principal fraudster to the financial system; this chapter unpacks the findings of this study as they relate to how fraudsters acquire the knowledge needed to commit a crime. The chapter provides an account of how learning occurred in the cases analysed in this study. It notes that differences exist both between insider and outsider crimes, and importantly, before and after the formation of criminal intent.

This chapter is split into two sections dealing with insider learning, outsider learning and a discussion section. Although the case data outlined in Chapter 5 originate from two police forces, and the cases themselves represent many different types of fraud, they are sufficiently similar that differences in the jurisdiction and fraud type were negligible. The

presence of similarities and differences based on proximity to the financial system made it possible to group emerging themes in new ways and shed light on specific processes.

The first section in this chapter focusses on learning from an insider's perspective by drawing on key themes identified in the case management files. Each theme is then broken down into temporal micro sections, each representing a different phase of the crime event; for instance, pre-crime to post-crime phases. This captures variation in the way fraudsters approach their learning at different phases of their crimes. The second section focusses on learning from an outsider's perspective. This section also breaks the analysis into a series of temporal micro phases to capture and depict variation in how outsiders learn in different phases of their crimes.

7.1 Learning and the Insider

A characteristic of the insider fraudster is their 'knowledge of [organisations] vulnerabilities and procedures, [which] could be used to cause significant damage to the business' (Australian Government, 2016, p. 17). However, few studies have considered the required level of knowledge needed to commit most frauds (Ayling, 2009; Hataley, 2020), with some exceptions such as hacking (Carnegie Mellon University, 2012; Ortega, 2006; Zhang et al., 2015). What literature does exist seldom considers how that knowledge was acquired outside assumed positions like learning via occupational positions (Katselas, 2018; Williams, Levi, Burnap, & Gundur, 2019). The Centre for the Protection of National Infrustructure (2013) found that a failure to apply 'need to know' control principles allowed insiders access to information to which they would not normally be entitled in their role, which conflicts with the more general 'need to share' principle that has become the mainstream in modern organisations (Best, 2011).

Some researchers make specific mention of the importance of knowledge to criminal groups. For example, in an examination of criminal organisations, Ayling (2009, p. 192)

suggested '[c]riminal organizations learn in the same way legitimate organizations do but face additional challenges'. Similarly, Hataley (2020, p. 658) contended that 'TOC [Transnational organised crime] groups are not unlike any other groups; learning has to take place and that takes place over time—TBML [trade-based money laundering] skills have to be transferred between groups and learned'. While such studies have identified the relative importance of learning, there remains a need to consider how knowledge and skills are acquired outside the assumption that all that is required is the acquisition of learning via daily routine activities (Ekblom & Tilley, 2000; Williams et al., 2019). Even in relation to crimes where knowledge is critical, like insider trading, research has generally failed to describe that learning beyond the fact that it arises through work opportunities. For example, Acharya and Johnson (2007, pp. 110-111); Biggerstaff, Cicero, and Wintoki (2020, p. 21); Katselas (2018, p. 113) all drew on a combination of news media and private information as sources upon which insider traders rely.[150] While the role of learning is usually acknowledged, its manifestation across different criminogenic settings, particularly where it relates to the crimes of insiders, remains under-researched (Ayling, 2009). Therefore, this chapter explores the learning opportunities exploited, and determines whether there are any temporal patterns in the steps to crime implementation.

As shown in Table 10, of the five analysed cases in which principal fraudsters were classified as insiders, four had associate offenders to draw on.[151] This suggests that any learning that took place during interactions between fraudsters occurred under social learning conditions, as alluded to by differential association theory (Sutherland, 1933) and later by social learning theory (Akers & Sellers, 2011). Table 10 also identifies two types of insider

[150] Acharya and Johnson (2007) examined variations between positive and negative news reports on the outcome of insider trading. Biggerstaff et al. (2020) described how the duration of an informational advantage derived from private information would impact the temporal placement of insider trades. Katselas (2018) examined the extent to which legitimate insider trading in Australia is information driven.
[151] Case 04 / Case 08 / Case 09 / Case 13

learner (Allan, 2018): the internal master and the internal learner. The internal master represents the 'highly experienced and knowledgeable insider with high levels of access and mobility across their respective organisations' and it is this group's mastery that enables them to commit their crimes within their respective organisations (Allan, 2018, p. 41). Conversely, the internal learner is 'generally [a] more junior or less experienced insider who, having lower levels of knowledge and freedom of access, ha[s] to actively seek out the knowledge necessary to commit their crimes' (Allan, 2018, p. 41).

Table 10

Insider Case Data

	Insider/outsider status					Learning source			
Case	Principal fraudster insider	Associate fraudster insider	Associate fraudster outsider	Internal master	Insider learner	Formal qualifications	On-the-job learning	Collaboration	Trial and error
04	X	X	X	X			X	X	
08	X		X	X		X	X	X	
09	X	X			X	X	X	X	
10	X			X		X	X		
13	X		X		X	X	X	X	X

X – indicates a positive correlation between the χ-axis and the γ-axis

Table 11 combines all the insider case data to provide an overview of how the insiders acquired the knowledge and skills necessary to commit their crimes. The table is split into three phases to represent the phases of learning identified along the fraud event timeline. Phase one identifies the learning period before the formation of criminal intent. Phase two identifies the learning that takes place following the formation of criminal intent, but before

the implementation of the crime. Finally, phase three identifies the learning that takes place following the commission of the crime or—in the case of ongoing crimes—the learning that takes place following the first iteration. When combined, these phases provide a comprehensive overview of how learning needs are satisfied at different phases of the internal fraudster's crime.

Table 11

Learning Phases and Insiders' Criminogenic Knowledge Acquisition

Insiders				
Pre-intent learning	Intent formed	Pre-crime learning	Crime phase	Post-crime learning
Qualifications Current and previous roles		Current and previous roles Collaboration Trial and error		Collaboration

7.1.1 Qualifications

7.1.1.1 Pre-intent Learning

While the influence of qualifications on criminal learning, particularly higher education qualifications, has historically remained on the fringe of criminological discourse, their association with learning theories has meant they occasionally feature in the literature (Association of Certified Fraud Examiners, 2014). In four of the five insider cases in this research, the principal fraudsters were found to have higher education qualifications.[152] In two of those cases, qualifications were considered prerequisites for access to the occupational positions held by the principal fraudsters.[153] In the other two, the fraudsters held higher education qualifications despite there being no occupational role requirements for them.[154] In

[152] ibid
[153] Case 10 / Case 13
[154] Case 08 / Case 09

the remaining case the principal fraudster held no higher education qualifications, nor did the occupational position require the holder to possess them.[155]

Some studies have found that the higher the education level, the more costly the fraud (Association of Certified Fraud Examiners, 2008), but not all studies have made the same connection between higher education qualifications and a tendency to commit fraud (Harbinson, 2020; Wheeler et al., 1988). What Cases 10 and 13 suggest, however, is that an absence of specific qualifications is likely to preclude someone from undertaking employment in a particular organisational setting. For example, PF10 in Case 10 was a qualified accountant and through this role he committed his crime. As identified by Detective N13, principal fraudster PF13 and associate fraudster AF13 both possessed higher education qualifications, without which they would not have held their occupational positions: 'He had a good understanding of the financial markets through his employment and through his degree at Monash University. He was third or fourth in his year at Monash and he got some awards, so he was really smart'.

Viewed from this perspective, it can be considered that aside from potentially offering a degree of knowledge that might be useful in a criminal endeavour, higher education qualifications are also prerequisite tickets for access, rather than just knowledge sources: for example without a qualification a lawyer cannot defend their client.

The data also reveal that not all of the fraudsters possessed higher education qualifications. This was true of the principal fraudster in Case 05 and the associate fraudsters in Case 08. In the absence of higher education qualifications, the principal fraudster in Case 04, the theft by a union employee case, worked his way up within the victim organisation throughout his 28-year career until he reached the equivalent of a CEO position. Over that

[155] Case 04

time, he developed a detailed understanding of the workings of the organisation, its strengths and its weaknesses. As noted by Detective N04:

> I think he was fairly well educated, but I wouldn't say, I don't think he went to university or any higher-level education as far as I am aware. Certainty he wasn't stupid by any means, he learned as part of his roles.

Similarly, in Case 08, the fleet vehicle procurement fraud, principal fraudster PF08 built his capacity over years of experience while also drawing on a syndicate that included three co-offenders, two of whom also held no qualifications beyond high school. This identified that the four criminal syndicate members—all professionals working across two international organisations and one national organisation—for the most part acquired their knowledge of the internal workings of their organisations and the target financial system throughout their respective careers (Carnegie Mellon University, 2012).

Rather than suggesting higher education qualifications were prerequisites, the data reveal that half of the principal and associate fraudsters in the insider group held no higher education qualifications. Instead, they rose to equivalent occupational positions as those holding qualifications. Nonetheless, in two cases an absence of a higher education qualification would have prevented the fraudster from accessing the financial system they targeted.[156] This suggests that while occupational positions might be a requirement to commit some forms of white-collar crime, the same cannot be said for the need for higher education qualifications in all instances.

A key finding was that qualifications as an active source of learning were only relevant up until the formation of criminal intent. This was unsurprising as would-be fraudsters are unlikely to enrol in a higher education program so they can commit fraud upon completion. Second, once criminal intent formed it was apparent that other factors began to

[156] See Cases 10 and 13

drive information needs, including a desire to remain undetected throughout the crime period—something that higher education qualifications are unlikely to assist with. Finally, there was no evidence in the data to indicate that higher education qualifications were a realistic source of information in the second, third and fourth learning phases; that is, the pre-crime, crime and post-crime learning phases.

7.1.2 Current and Previous Roles

7.1.2.1 Pre-intent Learning

Closely aligned to routine activity theory is the premise that an insider's role provides them with the knowledge and skills needed to commit a financial crime. In every insider case in this study, principal and associate fraudsters drew expertise from a combination of on-the-job learning, employment induction and in-house training sessions. The fraudsters had worked for their employers for between 3 and 35 years, with a mean length of service of around 18.5 years. This suggests that they were highly experienced operators within their respective organisations. Most of the learning throughout their employment was likely to have been legitimate, because the offences in question were of relatively short duration and it is unlikely that a motivated insider would wait 18.5 years to offend. As noted by Detective N10:

> Look, I guess it's just through his [job], as an accountant they become qualified, they learn those sorts of systems and what's involved, I guess he had that so much experience in the banking industry through his own practice that he knew what was involved.

Legitimate employees interact in known ways with known systems that are designed to effect outcomes. However, in only one case did the principal fraudster rely solely on their legitimate learning activities drawn from their daily interaction with the systems with which

they worked (Smith, 2014).[157] In all other cases, the principal fraudsters needed information not readily available to them through their occupational roles (Smith, 2014).[158]

7.1.2.2 Pre-crime Learning

A non-traditional method of occupational learning was described by Detective N09 in Case 09, the theft by a telecommunications company employee case:

> He's got his own set of credentials for all those systems, by telling people he needed them for his fraud investigations work … He went way beyond what he needed to get himself a set of credentials, which enabled him to use those systems. So, he a) got access and b) got himself trained.[159]

In this crime, PF09 was employed as a fraud investigations manager, and tasked with leading a fraud investigation team that investigated staff and customers who committed fraud against the organisation. In this role, PF09, a former fraud squad detective, investigated the criminal actions of others. Over time, he began to assess and refine those techniques before implementing improved versions of the crimes himself. As described by Detective N09, this exposure to criminal methodologies through employment, combined with prior occupational knowledge and an ability to analyse, reflect, and refine the mistakes of others, aided him in committing his crimes:

> So, I had actually found some of those facts sheets he had prepared for [the fraudsters he had investigated]; subsequently, they were found guilty in court and sentenced. But he was also committing [those] offences, he was learning what they were doing, and he was doing the same thing.[160]

[157] Case 10
[158] Case 04 / Case 08 / Case 09 / Case 13
[159] Case 09 Detective N09 Transcript
[160] Experiential learning suggests learning is the result of an individual's experiences (Kolb, 2014). Whether those experiences are created in classroom environments or arise in criminal settings is irrelevant given in either setting the process of attempting, failing, reflecting, and trying again results in an improved performance.

Another example of pre-crime learning drawn from Case 09 is the active exploitation of workplace relationships by principal fraudster PF09. As described by Detective N09, when he needed access to restricted systems, he would sweet-talk other staff members into facilitating this:

> That's what his defence was, he kept telling me he didn't know how to use those things [procurement systems]. But I had evidence otherwise. I've got evidence of him seeking outside the normal chains, sweet-talking girls etc., who sent him training material [on the procurement systems].

Pre-crime learning, based on knowledge derived from current or previous occupational positions, was also observed in Case 04, the theft by a union employee. While tendering to produce an annual publication, PF04 met AF04e, the proprietor of a printing company who quoted a job at AU$9 plus GST per unit, see footnote 83. However, as PF04 had in the past approved payments up to AU$20 plus GST per unit for similar jobs, he knew uncomfortable questions at audit time would be asked. Therefore, to evade questions over his previous contracts and continue defrauding his employer, he forced AF04e to agree to the same terms, those being AU$20 plus GST per unit.[161] This was agreed to by AF04e and the victim organisation's procurement manager AF04a, who was engaged in an extramarital affair with PF04. The agreement, according to the AF04a resulted in PF04 stating:

> We can all make a penny out of this. I want you to put this price on the job. I want you to double the price and you can keep 50% and the other 50% will be split between [the procurement manager] and I. I want the money paid to us in cash.

This indicates fraudsters will draw on knowledge from a range of sources by including previous deals, internal oversight controls and, in the case of urging illicit payments to be made in cash, the need to obfuscate the criminal distribution of funds in a way that

[161] Case 04 Statement-AF04e

lessens the chance of detection. This approach, of keeping the transaction off the victim organisation's books, also makes it harder for investigators to follow the money—something this fraudster was aware of.

7.1.3 Collaboration

7.1.3.1 Pre-crime Learning

After the formation of criminal intent, collaboration as a source of learning was a major contributor to the development and refinement of knowledge and skills. Collaboration was evident in all cases except Case 10, where the accountant acted alone. In the remaining four cases, the collaboration came in the form of internal collaboration between two employees,[162] and external collaboration between fraudsters inside and outside the victim organisation.[163]

The literature focusses on what brings collaborators together (Weerman, 2003). This may be 'individual-serving bonds', 'organisation-serving bonds' or 'affective bonds' (Free, 2015). However, complex crimes often blend several human and physical resources (Ekblom & Tilley, 2000, p. 387). The potential diversity of crime types suggests the nature of collaboration is likely to differ between cases as information needs are largely dependent on the specific circumstances found across different organisational settings. An example of collaborative pre-crime learning was observed in Case 13, where principal fraudster PF13 worked as a trader for a large Australian financial institution. In this role, he had developed a detailed understanding of a process known colloquially as 'news trading'. To augment this, PF13 as described by Detective N13, had also undertaken independent research outside his organisation through other commercial entities, to acquire as much skill as possible:

[162] Case 09
[163] Case 04 / Case 08 / Case 13

> From what we uncovered he had enquired with other brokerage firms around that same time but never actually opened up accounts and he did have to do those initial trades which were rubbish, in his own account, just to get an understanding of how the phone app worked so he could do it at work.

Supplementing the principal fraudster's activities was AF13, a school friend who worked for an Australian Government department whose data releases had a measurable impact on the Australian Stock Exchange. He provided this to PF13 in advance of its public release to allow PF13 to predict in advance the impact the data would have on markets prior to release, thus making short trades to their advantage. As described by Detective N13:

> But by all accounts, not one side had all the information, [AF3] knew and they spoke about it before committing the offence … they spoke about what information [AF13] had access to and what it means to the market and how it can affect it … Whereas [PF13] had a good understanding of foreign exchange … they worked out that they could probably make some money out of this.

This unique case provides an excellent example of pre-crime collaboration where, as a result, information deficiency was overcome through the combination of knowledge and skills possessed by separate members of the criminal syndicate. Therefore, collaborative pre-crime learning was triggered by a desire to commit an initial offence, although collaboration also occurred during the post-crime learning phase.

7.1.3.2 Post-crime Learning

In Case 08, the criminal syndicate had been operating a corrupt payments scheme linked to a fleet vehicle procurement fraud, initially between three companies and then two, over 10 years. The parties involved were the victim organisation, a fleet company that managed the fleet contract for the victim organisation and a consultant who arranged for the supply of vehicles to the victim organisation on behalf of the fleet company. Following an

agreement in principle by the victim organisation to source its vehicle fleet through the fleet vehicle company, the consultant AF08a who had organised the deal told AF08c and AF08d at the fleet vehicle company he expected a commission based on a per-vehicle, per-month figure of AU$30, which was in line with normal business practices. Soon after this, PF08 learned of this agreement and demanded half the payment for himself if AF08a and the fleet vehicle company wanted to keep the contract. This was despite the fact he worked for the victim organisation and would essentially be receiving corrupt payments funded by his employer. AF08a, AF08c and AF08d restructured the payments to a one-off AU$1,000 per-vehicle payment, half of which went to PF08. Over the years this scheme ran, AF08a, AF08c and AF08d continually restructured the deal after each fleet flip to ensure PF08 continued to receive his corrupt payment[164] and they, the business of the victim organisation.

Over time as legitimate contracts were restructured, the syndicate adjusted their method of offending to ensure it remained undetected by the victim organisation and others in the fleet company. To achieve this, AF08c and AF08d in the fleet company used their knowledge derived from their legitimate occupational positions to manipulate systems and records. As noted by Detective N08:

> There's no complex computer work that's happening, there's no identity theft or anything like that. It's just manipulation by people who are being told what to do, so they manipulate it to get the money. That's just the systems that are manipulated and then once that money is obtained then there's a lot of manipulation of the general accounting systems to either accrue that money or to get that money to the ultimate goal of where they are trying to get it to.

[164] A fleet flip occurs at the end of contractual cycle and results in the entire fleet of company vehicles being replaced with a new model.

This process of responding to structural changes in the legitimate deals that existed between these organisations put pressure on PF08 and his associates to ensure they were not detected. As noted by Detective N08, on one occasion associate fraudster AF08d told associate fraudster AF08c, 'No, dunce, you can't have your name on it. You need to create a company, back-date it to the time when these payments were supposed to start, and you can't be anywhere on the paperwork'.

Another example of post-crime collaboration is provided by Case 04, the theft by a union employee. Following the execution of search warrants by police at the residential addresses of PF04 and associates, they met to discuss and share their experiences of what had occurred. This sharing of knowledge was driven by the principal fraudster who sought to control the flow of information outside the syndicate, and to minimise his chances of prosecution. For example, PF04 shared with an associate advice he had received from a legal representative:

> when they [police] were in there cleaning out, taking boxes out of your place they would have been putting bugs in your house somewhere. Okay, so don't start having conversations about you know, start going for walks around the block, if you want to talk, okay and um just be ultra, ultra-cautious.[165]

Other examples of post-crime collaborative learning were evident in Case 04 where PF04 probed AF04c about whether police had asked her about who her accountant was:

> PF04: You didn't give them this other bloke's name [accountant]?
>
> AF04c: No, no because we weren't, we brought everything back here. But they [police] weren't really interested in going and talking to [accountant's name] um because they were interested in what we had there, and they were very specific about the time period they wanted.

[165] Case 04 LD Transcript – Café

> PF04: Yeah, no, okay, clean up … rake up the leaves in the yard. Rake up leaves like you normally do put it [records of business transactions missed by police during the search warrant] in there.[166] Ah just get three or four bags of leaves and shit and go off to the tip.[167]

Similar behaviours were seen in Case 08 involving fleet vehicle procurement fraud. Police officials arranged for PF08's new line manager to call a meeting with his associates at the fleet company, at which PF08 and two associates would be present. Lawfully acquired surveillance intercepts picked up extensive telephone calls between syndicate members discussing what might be said during the upcoming meeting. Through this interaction, the syndicate members discussed, assessed, discarded and finally settled on a common storyline to which they would stick, to justify the ongoing corrupt payments. As Detective N08 noted:

> How it actually flowed was we had arranged a covertly recorded meeting between [the victim organisation] and [fleet company]. It suited for that to happen because the management structure at [the victim company] had recently changed. So, the new manager of [principal fraudster PF08] hadn't met [the associates in their roles at the fleet company]. So, in the lead-up to that meeting we captured a lot of collusion between [associate fraudster AF08c] and [the principal fraudster PF08] in the planning of what was going to be said in that meeting, 'This is what we say, this is why we say it. If he asks this then this is what we say'. They even had their scare tactics of, 'If he asks this or pushes too much, we say this, and we are going to charge you this much'. There was a lot like we are talking hours and hours over a week-long period of constant, 'This is what we are going to do'. So, the meeting goes well, goes to plan, it's basically scripted as per the phone calls of collusion before it.

[166] Following the execution of a search warrant on the residential property owned by AF04d and AF04e, PF04 advised AF04d on ways in which she could destroy incriminating records that Police missed during this search of the property.
[167] Case 04 LD Transcript – Café

This aspect of the syndicate's activities is addressed further in Chapter 8, which concentrates on the planning behaviours of fraudsters. However, the extent to which these fraudsters committed time to the process of preparing, planning and memorising a variety of contingency stories points to the presence of a heightened level of post-crime learning. Apart from Case 10, the accounting fraud, data from all insider cases identify an increase in information seeking after the commission of the crime, which most cases was focussed explicitly on activities that helped to distance the fraudsters from the crimes they had committed. As shown in Table 10, OPSEC activities were undertaken by syndicates to remain undetected or to reduce the likelihood of prosecution if detected. These activities involved frequent and ongoing discussions, and sharing of knowledge, experiences and observations of police investigations.

7.1.4 Trial and Error

7.1.4.1 Pre-crime Learning

In the absence of direct and relevant experience, fraudsters like non-fraudsters may sometimes adopt a trial-and-error approach to overcoming obstacles. For example, Detective N13 described the activities of PF13 and AF13. In this insider trading case, PF13 and AF13 spent time planning, testing, failing, learning and then planning again in cycles towards the preparation of their crime. As Detective N13 noted:

> It was about identifying how to beat the system or possibilities of how to beat the system, then it was about working out what was needed to beat the system. Then it was about trial and error, then it was actually putting it into a plan and then putting the devised plan of how to actually circumvent it and do it well into action and then escalating it.

In one instance, as Detective N13 noted, PF13 and AF13 decided to undertake a so-called dry run to check whether they had everything in place they needed:

> Before there was any trading actually done, they did a trial run so, well actually [AF13] was meant to ring up [PF13] and let him know what the information was before the release happened but didn't for some reason; he puts it down to being a bit gun-shy. [PF13] rings him up and says, 'What's the information?' and he's like, 'Sorry I forgot about it. Just tell me what you get on your end'. So once the release is made, they ring and compare the information that [AF13] can get out of the computer as opposed to what was actually released and obviously it works out.

This collaborative process of devising a crime, testing it to identify irregularities and reflecting on the outcome of the trial run was unique among the insider cases, but more common in the outsider cases as explored in the next section of this chapter.

7.2 Learning and the Outsider

Motivated fraudsters operating externally to the organisational systems they exploit are faced with challenges in satisfying knowledge deficiencies over and above those faced by insiders. For the insider, knowledge of a potential opportunity might arise through their routine daily activities (Cohen & Felson, 1979). For the outsider, however, this knowledge, along with knowing how the system operates normally and what controls are in place to prevent breaches is crucial. Indeed, knowing how the controls in question respond to breaches, and how those controls can be overcome to facilitate access to the system in a manner that minimises the chances of detection, is important to the fraudster.

Limited access to the internal workings of systems, coupled with an absence of procedural knowledge, presents challenges for the outsider who, in most instances, cannot rely on personal access to an occupational position. Therefore, to navigate an increasingly diverse knowledge landscape, successful fraudsters gather information resources through a range of alternative means. Available avenues include dark web forums (Lane et al., 2020), criminal facilitators (Levi et al., 2005) and the subversion of insiders (Kendall, 2004). Some

have also been shown to deliberately seek positions of employment with victim organisations in the execution of their crime (Hutchings & Holt, 2015).

The exact form that learning takes differs between insiders and outsiders.[168] The data revealed that outsiders are less likely to hold higher education qualifications than insiders and the qualifications they do hold will not generally provide them with access to either systems or victims. The way in which their learning occurs, however, is similar to that of insiders. Insiders, like outsiders, learn through processes referred to as métis and techne (Kenney, 2010a). For outsiders, examples of métis include learning from previous experiences, trial and error, and collaboration. However, techne is more likely to be observed in instances where criminal facilitators instruct criminal syndicates on aspects of a new crime, or technicians instruct syndicate members in complicated coding practices. Whatever the approach adopted, outsiders enter periods of sustained knowledge acquisition to gain access to the systems knowledge they require.

[168] This is not to suggest that insiders and outsiders are cognitively different in any respect. Rather, that which they rely on in their learning is likely to vary from each other.

Table 12

Outsider Case Data

	Insider/outsider status					Learning source								
Case	Principal fraudster outsider	Associate fraudster insider	Associate fraudster outsider	Internal master	Internal learner	Formal qualifications	Current and previous roles	Collaboration	Criminal facilitators	Trial and error	Subverting insiders	Research	Law enforcement products	Criminal past
01	X	X		X		X	X	X			X			
02	X		X					X				X		X
03	X		X				X	X			X	X		X
05	X		X					X					X	X
06	X		X			X		X	X		X	X		X
07	X		X				X	X						
11	X	X	X		X	X	X	X		X				X
12	X	X	X		X		X	X	X	X	X			X

X – indicates a positive correlation between the χ-axis and the γ-axis

The second dataset examined in this chapter consists of eight cases where the principal fraudsters were classified as outsiders (see Table 12). Three of those cases relied heavily on the presence of subverted insider associates,[169] seven on outsider associates,[170] and two involved a combination of both insider and outsider associates.[171] This means that in only three of eight cases were some or all the information needs met through direct contact with the organisation,[172] which suggests that the remaining five cases did not reflect Sutherland's (1933) differential association theory explanation of learning via significant others in occupational settings. Additionally, as with the insider cases, there was evidence of both insider masters[173] and insider learners being used as information sources (Allan, 2018).[174]

Table 12 provides a high-level overview of the approaches taken by fraudsters in their search for relevant criminogenic knowledge, and Table 13 introduces a set of nuanced themes that emerged from the outsider cases. However, while three phases of learning were identified across the insider fraud event timeline (Table 11), the outsider data reveal four phases (Table 13). Phase one is the learning period before the formation of criminal intent. Phase two is the learning that takes place following the formation of criminal intent, but before the implementation of the crime itself. Phase three, not evident in the insider data, involves learning during the crime event itself, while phase four includes the learning that takes place following the commission of the crime or—in the case of ongoing crimes—following the first iteration of the crime being implemented. In combination, these four phases provide a comprehensive overview of how learning needs are satisfied during the different phases of the outsider fraudster's crime.

[169] Case 01 / Case 11 / Case 12
[170] Case 02 / Case 03 / Case 05 / Case 06 / Case 07 / Case 11 / Case 12
[171] Case 11 / Case 12
[172] Case 01 / Case 11 / Case 12
[173] Case 01
[174] Case 11 / Case 12

Table 13

Learning Phases and Outsiders' Criminogenic Knowledge Acquisition

Outsiders				
Pre-intent learning		Pre-crime learning	Crime phase	Post-crime learning
Qualifications Current and previous roles Criminal past	Intent formed	Current and previous roles Collaboration Trial and error Subverting insiders Research Criminal facilitators	Law enforcement products	

7.2.1 Qualifications

7.2.1.1 Pre-intent Learning

As with the insider cases, higher education qualifications were identified for some outsider fraudsters, although less frequently than for insiders. While principal fraudsters in four of the five insider cases held higher education qualifications, only three of eight principal fraudsters in the outsider cases held higher education qualifications.[175] Qualifications were considered a prerequisite for occupational positions in only one outsider case.[176] In this instance, Case 01 these were held by AF01a and AF01b, the subverted insiders who facilitated the principal fraudster's access to the organisational systems. In a second case, higher education qualifications provided direct technical knowledge and capabilities that the associate fraudsters used to hack POS devices and systems.[177]

Analysis of Case 05 provided no indication of whether the principal or associate fraudsters held higher education qualifications.[178] However, given similarities with Case 06

[175] Case 01 / Case 06 / Case 11
[176] Case 01
[177] Case 06
[178] Case 05

where high-level technical knowledge and skills were apparent, it is likely that some members of the Case 05 syndicate also possessed such knowledge and skills. Higher education qualifications were also present in Case 11, again held by an associate fraudster, although these qualifications had no bearing on the crime.[179] Thus, in three of the eight outsider cases (Cases 01, 05 and 06), higher education qualifications were viewed as instrumental in the fraudsters gaining access to organisational victims and providing a foundation upon which the requisite technical knowledge needed to implement a part of a larger fraud was built upon.

Higher education qualifications were in all cases acquired before the formation of criminal intent. This added weight to the findings from the insider case data analysis that higher education qualifications are not a major determinant of whether a high-value fraud will be successful (Association of Certified Fraud Examiners, 2008). The principal fraudsters in most outsider cases did not hold higher education qualifications; rather, high school education was the most frequently cited highest education level.[180] This finding is similar to that in a study by Wheeler et al. (1988) where 79.3% of fraudsters had finished high school but 72.9% had never completed higher education studies.[181] Professional practice experience developed over years accounted for the level of knowledge demonstrated by the principal fraudsters and their associates in the current study. As Detective N02 in the account takeover fraud noted, 'Yeah, most of them are just high school, that's about their highest level of education and after that it's maybe a few dead-end jobs and then they are straight into this sort of thing'.

In the absence of professional experience, some fraudsters augmented their knowledge deficiencies via subversion or recruitment of insiders and technical specialists

[179] Case 11
[180] Case 02 / Case 03 / Case 05 / Case 07 / Case 12
[181] Drawing on US Court data Wheeler et al. (1988) set out to establish differences between white-collar criminals and what the deemed were common criminals.

who themselves held higher education qualifications. The data suggest that in Cases 01 and 11 those qualifications were only relevant to obtaining useful occupational positions, whereas in Case 06, that knowledge was directly relevant to the crime. Although recruited knowledge made up a significant portion of the outsider case data, in most instances, knowledge arose in different domains. Therefore, as with the insider cases, the outsider cases demonstrate that higher education qualifications were not a prerequisite in these fraud cases. Indeed, outsiders rose to occupational positions equivalent to those that held higher education qualifications. While some cases satisfied this need through the subversion of insiders who held positions that did require higher education qualifications, they were in the minority. Most cases instead demonstrated that the necessary knowledge and skills came from various domains outside higher education.[182]

7.2.2 Current and Previous Roles

7.2.2.1 Pre-intent Learning

Like insiders, outsiders also drew on previous occupational positions as sources of learning. Indeed, knowledge and skills obtained through previous and current employment were evident in five of eight cases.[183] In three of those five, knowledge was drawn from subverted insiders as addressed later in section 7.2.6,[184] and in the other two, it was gained through previous employment[185] and current occupational roles.[186]

7.2.2.2 Pre-crime Learning

Case 01 provides a good example of learning via current roles: in this case, the two associate fraudsters, AF01a and AF01b, were considered internal masters because of the heightened level of expertise held by these insiders.[187] A further two cases, Cases 11 and 12,

[182] Case 02 / Case 03 / Case 05 / Case 07 / Case 12
[183] Case 01 / Case 03 / Case 07 / Case 11 / Case 12
[184] Case 01 / Case 11 / Case 12
[185] Case 03
[186] Case 07
[187] Case 01

were described as internal learner cases because of the relative inexperience of the insiders, which was evident in the level of learning they had to undertake during the pre-crime learning phase.[188] In Case 01, previous and current employment provided the subverted insiders with all access and information needed to commit the crime. The two subverted insiders had a combined 9 years of senior executive experience with the victim organisation, classifying them as internal masters. As noted by Detective N01:

> They had high levels of specialist knowledge, this was a fraud against the procurement process, and they were highly involved in the procurement of software for the enterprise, multimillion-dollar contracts, highly experienced in how it worked and what they were supposed to do, their knowledge, that was their job, that was how they get these jobs.

Their expertise was significant as they had decades of previous employment in the field before joining the victim organisation. Their exploits were aided by their capability as effective operators and the level of trust placed in them by senior management. Indeed, one of the two associates was responsible for maintaining standards and ethics in their department via the enforcement of a gifts register. As Detective N01 noted:

> we've got all the evidence of him enforcing the gifts policy. He maintained a conflict-of-interest register, he put his own gifts on it, (Detective N01 speaking in second-person voice) 'I'd better write on there I spoke to someone who was married to someone', but he didn't mention he got 2.5 million bucks off them, (Detective N01 again speaking in second-person voice) 'oh I did get a bottle of wine off Acer computers'; what about the 2.5 million bucks from [the principal fraudsters company]?

[188] Case 11 / Case 12

However, unlike Case 01, most cases involved more than one source of information. For example, in Case 03, the mortgage and finance fraud, principal fraudster PF03a relied on years of experience as a lender of last resort and finance broker to Sydney underworld figures (Australian Broadcasting Corporation, 2011; Campbell, 2006). PF03a combined his knowledge of property finance and financial systems; PF03b drew on connections within Sydney trade unions and the construction industry to identify opportunities; and AF03a used his experience in running businesses. When combined, these skills allowed this syndicate to operate effectively.

Pre-crime learning was also observed in a second mortgage fraud case, Case 11, the land valuation mortgage fraud. The initial idea for the crime arose during a discussion between the principal fraudster PF11 and his associate AF11a. Together they identified a need for additional information and skills and compensated for these deficiencies by reaching out to a second associate who identified an insider in the victim organisation. AF11a, the 'go-to document forger for all the top-end offenders for the last 20–30 years',[189] developed his expertise throughout his illegal career. This he combined with the knowledge of the financial sector that PF11 and other associates possessed, and the access to the target financial system provided by the third associate.

7.2.3 Collaboration

7.2.3.1 Pre-crime Learning

Collaboration was crucial to the success of the outsider frauds in this study and is, according to Ekblom and Tilley (2000), a resource given that some crimes require a combination of knowledge and skills that is beyond the capacity of an individual. While not exclusive to outsider crimes, collaboration accounted for a large proportion of the learning and information sharing activities in this dataset. Faced with several challenges posed by the

[189] Case 11 Detective N11 Transcript

sheer diversity found in finance systems, outsiders need to understand the function of the systems and the type of product each system manages. Additionally, different anti-fraud controls serve to protect different organisational systems. Consequently, a lack of access and familiarity with organisational systems poses a challenge to outsiders seeking to commit fraud. Collaboration, therefore, as a resource, brings together an array of knowledge, skills and expertise to aid in the completion of a criminal enterprise (Ekblom & Tilley, 2000).

Collaboration was evident in all eight outsider cases;[190] however, the most significant example of pre-crime collaboration was observed in Case 03. Here the fraudsters PF03a, PF03b and AF03a combined an array of personal, moral, cognitive and facilitative resources.[191] The crime, a series of loan and mortgage frauds predicated on the theft of OT03a's identity, entailed the creation of several fake business fronts with websites and Yellow Pages listings. All three offenders played specific roles, each bringing a different knowledge base and skill set. The principal fraudster PF03a was an experienced financial broker with knowledge of various financial products. He was responsible for managing the compilation of a range of supporting resources in the form of loan documents, falsified credit checks and fraudulent identity documents.

The principal fraudster, PF03b, with connections to the Sydney criminal underworld and its construction industry, had numerous contacts that provided potential opportunities and expertise to add a level of legitimacy to their fraudulent deals. This was observed in a conversation between the principal fraudster PF03b and one of his industry associates, AF03b, in a legally acquired telephone intercept:

> PF03b: I'm sitting down with the guy from [victim finance company] sometime this week; that finance guy…

[190] Case 01 / Case 02 / Case 03 / Case 05 / Case 06 / Case 07 / Case 11 / Case 12
[191] (Ekblom & Tilley, 2000)

AS03b: Yeah, yeah, yeah…

PF03b: I just wondered whether it might be a good idea if you were there…

AF03b: Yeah.

PF03b: …because we will say we have got the contracts, but you are managing the whole lot. You know overseeing it all, so it gives them more confidence in funding them, yeah?

AF03b: No problems mate, you just let me know what day and what time and I'll be there.

PF03b: Lovely, ok mate. I'll put it all together, I've got the pack ready for them, so um we'll get it funded ok, but ah we'll just need … so, your experience…

AF03b: Sorry?

PF03b: Oh well, I've got it funded and everything and the company we're buying it through is a construction company, but we haven't got any experience in the actual…

AF03b: Yep, yep, yep…

PF03b: …excavators, so we will say we are buying them we are going into excavation but under the, under you. We've got the contracts, but you'll manage it, oversee it for us.[192]

As the fake business front of the criminal syndicate run by PF03b had no credentials in the construction industry, PF03b recruited AF03b to be present at a meeting with the victim company's representative. The intention of this collaboration, this thesis asserts, was to satisfy any due diligence processes the victim heavy machinery finance company might conduct as part of their normal business process.

Meanwhile, around the same time, the syndicate members in Case 03 were also actively seeking to defraud a vehicle dealership. On this occasion, associate fraudster AF03a,

[192] Case 03 LD Transcript

the third member of this syndicate, brought a working knowledge of business operations and the various roles that existed across most organisations. Providing what is known as backstopping services, he used fictitious aliases when purporting to be the holder of numerous positions, including financial controller and office manager in the various fictitious organisations on which the finance frauds were based. The following conversation between the principal fraudster PF03a and AF03a was captured on a legally acquired telephone intercept, and recounts a conversation following a request by the victim vehicle dealership for additional information in support of that fraudulent vehicle loan application:

AF03a: Yo.

PF03a: Yeah, she said there's a couple of questions you didn't answer, and you haven't sent back the privacy form.

AF03a: Yes, I did, it all got sent, man.

PF03a: Can you just double-check, she said she hasn't got it. I was just talking to her thirty seconds ago.

AF03a: Because remember he was there, and we gave the number?

PF03a: What? Yeah, and what you—she just wanted a couple of questions and that's all she said.

AF03a: Fuck.

PF03a: Well, mate, she said she hasn't got the answers and she doesn't have the privacy form.

AF03a: But we gave her all the…

PF03a: Can you just fuckin' check and…

AF03a: Oh, that's right, no, no, remember, we left out the accountancy details.

PF03a: Yeah, can we sort it out now?

AF03a: (Unintelligible)

> PF03a: No, I didn't want her to go to the (unintelligible) no. No, um, okay, just send the privacy form back, and I'll fuckin' take over (unintelligible). I'm going to have to tell him. Have to go … just fuckin' send the privacy form, that's all and everything else.[193]

This discussion between PF03a and AF03a identifies the different roles played by two members of this criminal syndicate. PF03a acted as the public-facing applicant of the same fake business front used in the heavy machinery finance fraud, and AF03a performed an administration function. The intention of this collaboration, this thesis asserts, was to provide an appearance of legitimacy on the part of the fake business front so that it appeared that the syndicate's business had the required back-of-house administrative functions.

7.2.4 Criminal Facilitation

7.2.4.1 Pre-crime

Closely aligned to collaboration during the pre-crime learning phase was the criminal facilitative services provided by several criminals in two of the outsider cases. In Case 12, the superannuation fraud, the alleged internationally based mastermind behind the crime was a key contributor.[194] OT12a met PF12a and PF12b in Amsterdam, where he pitched the plan to them.[195] OT12a was then observed in Australia before both the trial run and the main crime; however, on both occasions, he flew out of Australia in the days leading up to both events to ensure he was not detained should the scheme be detected. As Detective N12 described:

> OT12a had left the country just before that happened, he did not want to be here when it happened … when he left the country, I think it was before the October long weekend, [Australian Border Force] did a search on him when he left the country and on him were a number of documents that included [the victim bank] documents …

[193] ibid
[194] Case 12 Detective N12 Transcript: OT12a was an internationally based criminal facilitator who police believed had been involved in similar crimes overseas.
[195] See (McClymont, 2012)

> [The crime] didn't happen and then he comes back in November, meets with the [principal fraudsters], there is surveillance by the NSWPF of him handing over envelopes, at the time they weren't sure what they were looking at, it turned out to be this fraud, but then OT12a leaves again before the [main crime] went down.

Similarly, in the criminal syndicate involved in Case 06, the card skimming case at service stations, the principal fraudster received training overseas from a more experienced operator, as described by Detective N06:

> PF06a(1) came into the country and actually just did spend offences, which is what the runners would normally do, running credit cards, and then left before we detected him … So, it's a big circle, he's then pissed-off out of the country, been trained up [by a more experienced criminal], then come back in as the man, top dog … came back as an international organiser.

7.2.5 Trial and Error

7.2.5.1 Pre-crime Learning

Like in the insider cases, the outsiders demonstrated periods of trial and error. Rather than simply 'making it up as they go', this trial and error involved instances where the fraudsters knew the exact nature of the obstacles they had to overcome. Internal learners in Cases 11 and 12 undertook periods of what is known as problem solving via trial-and-error learning (Marengo & Dosi, 2005). These subverted insiders built up their knowledge via a series of pre-crime dry runs where they tested the validity of their planning; like the way a researcher tests a hypothesis. In these cases, the subverted insiders had both access to and knowledge of how specific systems operated under normal circumstances. However, because of the nature of the crime and the presence of internal controls, the insiders undertook periods of trial-and-error learning to implement their crimes. For example, in Case 11 the land valuation mortgage fraud, fraudulently over-valued properties were used to obtain mortgage

loans that were paid into bank accounts controlled by the principal fraudster. In this case, the approval process at the victim organisation was automated. It relied on mortgage brokers working for the organisation to enter information and respond to several system-generated questions. When completed, this determined whether a physical property inspection was required to verify the value of the land. As noted by Detective N11, the subverted insider overcame this through a process of trial and error:

> on day 1 he puts a series of things in, and it generates a 'required valuation report' status. Then later that day he changes one or two of the answers for the same property and it generates another report. So, over 3 days he puts in seven different combinations and on the seventh he gets a 'no external valuation report required' status. Then every loan after that is done exactly the same to those questions. So basically, he worked out the system; he logged on but never finalised because he didn't get the outcome that he wanted. He goes back, thinks about it, has another crack and then eventually on attempt seven he got it and then each one thereafter.

The internal learner in Case 12 was the telecommunications technician introduced in section 6.2.4. While not employed by the victim organisation, his role as a telecommunications employee provided the criminal syndicate with the capacity to hack the telecommunication lines between the victim organisation and a funds management organisation that handled a portion of its daily trades. The hack enabled an associate to send a funds transfer request that would appear as if it came from the authorised funds management company, and arrive at the fund's holder organisation, prompting the transfer of AU$150 million into accounts controlled by the principal fraudsters. The internal learner practised this over 3 days, beginning 12, 4 and then 1 day out from when the fraud was to be executed. During this period a police facts sheet examined in Case 12 recorded:

> [The subverted insider] entered the Telephone Exchange on 12 December, 20 December, and 23 December. [He] had no work-related reason to enter the Telephone Exchange on 12 December, 20 December, or 23 December; and [he] accessed the exchange to make preliminary inspections of the premises and the MDF [main distribution frame] to facilitate the hacking of telephone exchange equipment and wiring on the 24th of December, the day of the crime.[196]

The combination of access to, and knowledge of, general organisational systems enabled the subverted insiders to build on their existing knowledge towards the manipulation of different organisational systems to the advantage of the principal fraudster. Understanding that subverted insiders have differing levels of expertise enhances understanding of both the role of these individuals in the criminal process and provides examples of how they were used.

7.2.6 Subverting Insiders

7.2.6.1 Pre-crime Learning

In the absence of legitimate access via employment or even via commercial interface points, fraudsters will attempt to subvert insiders. The subversion of insiders by outsiders in this study was evident in four of eight outsider cases.[197] This demonstrated that a combination of knowledge, access and technical skills was critical to the successful outcomes of these crimes. As Detective N03 noted:

> To perpetrate the crime, it's generally a cultivated person from the inside to commit the hack. It needs to be well thought out, they need to profile the person, work out their vulnerabilities and manipulate them. The sophisticated cases are well planned

[196] According to Detective N12, the syndicate planned to implement the crime on the 24th of December to take advantage of the usual practice of a boozy pre-Christmas lunch followed by several days of non-trading, all designed to give the syndicate more time to get away with their crime.
[197] Case 01 / Case 03 / Case 06 / Case 12

and require the motivation of their people. It is vital that you have an insider for the corruption to occur.

Across this dataset, several different approaches were adopted by principal fraudsters to subvert insiders. One involved initiating intimate relationships with bank managers who, having been ensnared by a syndicate member, approved fraudulent loans initiated by their partner, as described by Detective N03 in relation to the finance application fraud syndicate:

> They targeted vulnerable female bank managers; they drove all over Sydney to unique financial institutions to the chosen potential managers. These managers were in relationships with these corrupt brokers. The corrupt brokers formed part of the hierarchy of the organised criminal structure.

In another case, the syndicate members resorted to financial incentives as a way of subverting insiders. In Case 06 a syndicate skimmed the debit card details of thousands of victims using POS devices covertly installed in service stations across Sydney. They cloned the stolen card details onto blank cards and used them to withdraw funds from the victims' bank accounts. However, to initially skim the credit cards, the fraudsters needed some way of installing them in locations with high daily card volume usage—usually more than 400 transactions per day, per POS device. As described by Detective N06, the syndicate paid employees at selected service stations to enable this access.

> they did on occasions buy off the service attendants. They would often be Indian students working in the service stations, they would give them 20 grand to turn a blind eye for a couple of hours while they install or swap over or pull out [a POS] to compromise and then they turn a blind eye when they pull out again, so it is guaranteed they're in and out.

A final approach to the subversion of insiders was seen in Case 01, where two high-ranking executives in the victim organisation were gradually corrupted by PF01 over a

prolonged period. As initially described in section 6.2.2, the principal fraudster had built up professional relationships with the associate fraudsters over years. Predicated on this improper relationship the principal fraudster deliberately used the two associate fraudsters to gain their access, knowledge and loyalty. As Detective N01 noted:

> there is a pattern that he's played them like fiddles and at the end of this he's dumped them as he's done with many, many other people, he planned it. There is no question he planned it, his emails show that this is how he does business, he gets his people into other organisations whether they realise that's their role or not.

The deliberate and planned nature of this subversion resulted in a primary fraud of AU$14 million. A secondary fraud of US$263 million was deliberately engineered to the extent it was unlikely the two associate fraudsters were aware of how far they had transgressed. As Detective N01 noted:

> there was a lack of transparency when the executive general manager [AF01a] was employed, he was always the candidate from [the principal fraudster's organisation], so the [principal fraudster] was actively and clandestinely using him into that organisation. The whole thing is predicated upon improper relationships and I think as often happens with these improper relationships, it is not a question of (speaking in second-person voice) 'Ah look I got you that job where's all my stuff'. This was a slow seduction that goes on over a long period of time. They crossed the line so long ago they didn't realise they did it and when they looked back, they went 'holy hell look how far back that line is now' and once you've done, you're done. I don't think they knew they crossed the line; I don't think they intended to cross the line, but there's an inappropriate relationship, they think they are grown up enough to manage that inappropriate relationship, there's dinners, there's holidays, this tight close

relationship they have with these people, they genuinely seem to be friends with each other.

7.2.7 Research

7.2.7.1 Pre-crime

Research, as distinct from trial and error, describes instances of learning where syndicate members, already aware of their knowledge and skills shortcomings, identify avenues to overcome those deficiencies and set out to achieve that aim. There were examples in this study of principal and associate fraudsters interacting with entities to gain the information they needed. This included interacting with victim organisations using aliases to scope controls or opportunities. In other cases, it involved interacting with third-party organisations to build up the apparent legitimacy of the syndicate. For example, PF03a in Case 03 called OT03c, a customer service representative working for a company that offered virtual office services, to establish the cost of setting up a virtual office to backstop his syndicate's finance application frauds:

OT03c: Good afternoon this is [business name].

PF03a: Yo.

OT03c: Hello.

PF03a: Who's that?

OT03c: This is [OT03c], how can I help you?

PF03a: It's [PF03a], how are you going mate?

OT03c: Oh [PF03a], how are you going?

PF03a: Good, good, mate just quickly I wanted to ask you the, your box, the address there…

OT03c: Address, yeah?

PF03a: Yeah, how does that go? Go like in the um, [business suite name] something, or how do you use it?

OT03c: Um, if you want things to be sent here, all you need to write is Shop 1/20 [XXX] Street, Sydney, New South Wales, [XXX].

PF03a: Ok, and if you want to, ah, if you want a physical address or one of those boxes, what do you call those boxes? Have you got an address for each; do you have boxes?

OT03c: Yep, we do, we have boxes.

PF03a: What's the story there?

OT03c: For the boxes, all you need to add on the front for all those boxes is Suite number 104, or…

PF03a: What have you got? What have you got available; can you tell me?

OT03c: Hang on a sec … we have 115.

PF03a: 115.

OT03c: Hmm.

PF03a: And how much is that for a year?

OT03c: For a year, ok … is it personal or business?

PF03a: Um, well it will be business.

OT03c: Business, for business that would be $160.

PF03a: Ok, can you just, I'll come sort that out with you tomorrow.

OT03c: Alright.[198]

This and other research-related learning activities provided the syndicates with a range of genuine products and services that helped them project an air of legitimacy to backstop their fraudulent mortgage and loan applications. This gave them surety that due

[198] Case 03 LD Transcript

diligence checks undertaken by the victim companies would be met with a seemingly legitimate response. In this example, should a victim company conducting customer due diligence seek to check whether the listed company was real, the phone number supplied on the application form would go to a remote number answering service. This would then be diverted back to a syndicate member who, having a different identity linked to different phone numbers, would be able to identify which false identity to adopt depending on which number it came from.

Directed research was also evident in Case 06, one of the card skimming cases, and Case 02, the account takeover case.[199] In Case 02 the fraudsters had no education past high school. To commit these technical crimes the fraudsters undertook periods of internet research using the surface web via search platforms like Google, as well as several dark web hacking portals. As noted by Detective N02:

> We're dealing with a lot of younger offenders, they all are self-taught, through googling, none of these are guys who are computer science students, they are just people who have googled their way through finding gaps in the banking sector that they can exploit.

7.2.8 Law Enforcement Products

7.2.8.1 Crime Phase Learning

One final source of learning that was unique to the outsider cases—specifically, those that involved a series of ongoing crimes—was the output of police investigations. Police investigations produce numerous documentary outputs that are, by law, shared with the accused via their defence solicitor. The data reveal instances of fraudsters using police-generated reports as a trigger for learning and improvement, which is representative of stigmergic processes (Nieto-Gomez, 2016). One particular document generated by police is

[199] Case 02 / Case 06

referred to as a facts sheet. In addition to identifying the accused and their alleged crimes, it provides a detailed account of the evidence police will rely on should the matter proceed to trial. Such information products are often used by criminals to evolve their offending practices, as described by Detective N05 when discussing one of the POS skimming cases:

> One of the things we identified with this particular criminal as it wasn't our first interaction with him. His methodology and his understanding of the financial system has evolved, and we could clearly see it evolving.[200] He minimised his exposure to police, he became more aware of police methodologies, he learned from his previous mistakes. One of the things that are incumbent on the police to prove a case, is to provide the court with a facts sheet. When we first arrested this bloke, and it was exactly 1 day short of a year that we had previously arrested him so when we provide him with the facts sheet it will outline how we conducted this surveillance, we followed him to here, we saw him conduct these actions, we stopped, and we searched him, and we gathered all this. So, he learned from this facts sheet so that the next time he's not going to the same sorts of establishments that we arrested him at. He's changed his methodology to frustrate police investigation.

7.3 Summary

The analysis in this chapter has identified both similarities and differences between how insider and outsider fraudsters approached the acquisition of knowledge. Traditional learning sources including on-the-job learning opportunities, higher education qualifications, and knowledge, skills and techniques derived from routine daily activities provided most of the necessary knowledge in the insider cases. However, the learning undertaken by the outsiders was more diverse, as they drew on both traditional and non-traditional learning

[200] This is a point made by Hataley (2020) who suggested for criminal groups to survive they need to evolve and learning is at the centre of this premises.

sources. The data also reveal the presence of four distinct learning phases: pre-intent, pre-crime, crime and post-crime learning phases. The significance of the identification of these learning phases is that they facilitate the separation of pre-and post-intent learning behaviours, which was found to shape the manner of knowledge acquisition.

Qualifications were observed as a learning source in the pre-intent phase only, with principal and associate fraudsters holding these in just over half of the cases.[201] However, the relative capacity of higher education qualifications to satisfy the information requirements of frauds varied, with only 3 of 13 cases demonstrating them as enabling factors.[202] This suggests that while the insider case data identified greater levels of higher education qualifications than did the outsider case data, this should not be viewed as being directly relevant to all fraudsters who held them. Instead, as was more often the case, qualifications acted as prerequisites to employment in some professions. However, despite the popularity of linking educated white-collar workers and fraud (Association of Certified Fraud Examiners, 2008; Sutherland, 1947), the same level of access was achieved through the length of service and other non-qualification expertise in three of five of the insider cases.[203]

The second traditional learning source identified was on-the-job learning, which was evident in nearly all cases.[204] However, the nature of learning evolved across fraud event timelines. Pre-intent learning was characterised by both a lack of specific criminal intent and a more generic process of knowledge acquisition linked to an individual's role. However, following the formation of criminal intent, the learning became more deliberate and focussed, characterised by both criminal intent and the need to satisfy specific information needs linked to the implementation of the crime. Pre-crime learning occurred in a variety of ways. This included overt discussions with external suppliers who eventually became complicit in the

[201] Case 01 / Case 08 / Case 09 / Case 10 / Case 11 / Case 12 / Case 13
[202] Case 09 / Case 11 / Case 13
[203] Case 04 / Case 08 / Case 09
[204] Case 01 / Case 03 / Case 04 / Case 07 / Case 08 / Case 09 / Case 10 / Case 11 / Case 13

principal fraudster's crimes[205] and the sharing of information sourced from different organisations by co-offenders.[206] Fraudsters also used deception[207] or theft to extract knowledge and skills from others in their organisations during the pre-crime phase.[208]

Non-traditional learning sources were evident in the outsider cases. These included the subversion of insiders, the use of criminal facilitators, crime-related research and stigmergic learning episodes triggered by police intervention. Subversion was a common non-traditional method of overcoming information deficiencies in outsider cases. The activities of subverted insiders, however, varied. Linked to experience, some insiders, referred to in this research as 'internal masters', were highly educated and experienced insiders who provided the principal fraudster with all the relevant knowledge. Although other insiders with less experience were described as 'internal learners' and might have a general working knowledge of organisational systems, they had to undertake periods of self-directed learning to satisfy the information requirements. Another unique non-traditional learning example arose where a fraud investigator in Case 09 copied, refined and improved the frauds he was investigating and then implemented them himself to his financial benefit.

Finally, a significant amount of learning occurred across the post-crime phase in cases where syndicate members shared information following detection. This involved developing post-crime accounts by discussing and memorising common stories. This was evident in Case 04 where syndicate members spent prolonged periods discussing their interactions with investigators, including search warrants and interviews, all the while seeking to ascertain what police authorities might have found or missed.

[205] Case 04
[206] Case 13
[207] Case 09
[208] Case 04

Chapter 8: Tradecraft—Planning of Financial Crimes

Fraud is a series of micro events, some legal and others illegal, that are spread along a fraud event timeline with the formation of criminal intent defining the starting point. However, from an analytical perspective, identifying the formation of criminal intent as the actual start of a period of offending precludes from examination other factors worthy of analysis. Similarly, determining the end of a fraud event timeline is problematic. For example, if a fraud successfully nets the criminal a financial advantage, that might identify the end of the fraud event timeline. However, this would exclude post-crime activities such as destruction of evidence, creation of alibis and monitoring of police investigations. Therefore, while it is logical to suggest that a fraud event timeline unfolds in phases—commencing with the formation of criminal intent and ending when the fraudster makes an illegal financial gain—to better understand how frauds are committed, an examination of behaviours outside this convenient timeframe is necessary.

Setting popular fiction to the side, the presence of legislative wording like ‘Intention to defraud by false or misleading statement’ ("S192G Crimes Act," 1900) and ‘Conspiracy to defraud’ ("S135.4 Criminal Code Act," 1995) suggests that some fraudsters plan their crimes (Allen, 2011). Variables such as insider or outsider status also influence how and when fraudsters undertake their planning activities, as was the case with access and learning in the cases in this study. Planning involves considering factors like victim access and selection, deterrence measures, the likelihood of detection and risk minimisation strategies, while at the same time maximising potential gains (Bernard et al., 2016, p. 47). Such decisions are thought to be based on an assessment of costs and benefits, particularly subjective factors including fear of apprehension versus the thrill of achievement; and objective factors including formal punishment versus likely benefits gained (Benson & Simpson, 2018). This

cost–benefit analysis process is rooted in the theoretical underpinnings of rational choice theory (Cornish & Clarke, 1986).

This chapter presents an analysis of the differences in how insiders and outsiders plan their frauds. In a similar manner to previous chapters, this chapter relies on a fraudster's proximity to the organisational system as the variable shaping differences in insiders' and outsiders' tradecraft. As the final chapter aligned to the ALPi Model, this chapter acknowledges that planning will occur in more ways than can be addressed here. However, what this chapter achieves is an analysis of how criminal planning occurred across the cases that made up this study. The chapter is split into two sections. The first focusses on the planning behaviours of insiders by drawing together themes identified in the data and the second focusses on the planning behaviours of outsider fraudsters who, in the absence of a legitimate insider position of trust, cannot rely on traditional avenues used by insiders.

8.1 Planning and the Insider

Insiders have advantages not available to outsiders who are not privy to the same level of access to organisational systems. Insiders also enjoy the benefit that their role allows them to hide in plain sight. As such, they are more likely to have a working knowledge of how financial systems function and respond to illicit incursions, which underlines the connection between learning and planning. This includes the ability to search out weaknesses, and obtain password privileges and other material benefits available to an insider, thus providing a solid foundation upon which planning can commence following the formation of criminal intent.

The findings in this section are separated into three broad themes: planning triggers, temporal planning phases, and planned outputs, as set out in Table 14. The first, planning triggers, describes factors that trigger sudden increases in planning, which historically have related to environmental changes—that is, changes in procurement processes (Schroeder et al., 2014) or police intervention (Nieto-Gomez, 2016)—which the data here confirm and

support. The second sub-section, on temporal planning phases, describes the distribution of planning-related activities throughout the criminal process. Finally, the planned outputs sub-section describes how the planning intention of fraudsters manifests itself in terms of the actions they take.

Table 14

Insider Planning Data

	Planning triggers				Temporal planning phases				Planning and decision-making outputs				
Case	External factors	Detection of crime	Financial demands	Data release cycles	Pre-intent phase	Pre-crime phase	Crime phase	Post-crime phase	Delegate planning	Associate roles critical	Rehearsal and trial runs	Manipulation of others	Concealment strategies
04	X	X				X		X		X		X	X
08	X	X					X	X	X	X		X	X
09		X					X	X				X	X
10			X				X					X	
13				X		X	X			X	X		X

X – indicates a positive correlation between the χ-axis and the γ-axis

8.1.1 Planning Triggers

Planning is '[a]n organised and especially detailed method according to which something is to be done' (Stevenson, 2007, p. 2230). For insiders, the 'something' is fraud, and the 'method' is the way the fraud should be undertaken. The nature of planning in the insider frauds in this study did not directly correspond with levels of access and knowledge, as in most instances there was less planning early in the fraud event timeline. Instead, the distribution of planning across the case fraud event timelines varied, with planning becoming increasingly prominent once the fraud was underway. Cases 04 and 13 were the exceptions, with examples of pre-crime planning that followed the formation of criminal intent (see Table

14). However, what separates these two frauds is the way in which the planning occurred. For example, in addition to planning the mechanics of the crimes, in both cases the fraudsters considered the potential punishments their endeavours might attract and took active steps to limit the chance of this occurring.[209]

In the remaining three cases, the identification of an opportunity, combined with limited planning saw the fraud commence (Cromwell et al., 1991).[210] However, in all five cases, different factors triggered periods of planning during the crime[211] and post-crime phases.[212] The specific nature of the planning triggers varied. For example, some factors were foreseeable, such as the potential for detection, the end of procurement contract cycles and the regularity of data release cycles. However, other trigger events were unforeseeable, such as associates withdrawing from the criminal syndicate because of 'cold feet'.[213] Either way, these foreseeable and unforeseeable events triggered periods of reactive planning on the part of the fraudsters.

8.1.1.1 External Factors

Analysis of the insider data suggests external events are a common factor that stimulates periods of planning. External factors are influences that jeopardise the continuation of the fraud; for example, in Case 08 the external factor was the end of a contract. In this case, the principal fraudster PF08, the fleet manager at the victim organisation, received corrupt payments from the fleet company that held the contract, which was ultimately funded by the victim organisation. The externality was the ending contract, and changes to the victim organisation's oversight processes forced the syndicate to devise new methods to defraud the

[209] Case 04 Participant Transcript and Case 13 Participant Transcript
[210] Case 08 / Case 09 / Case 10
[211] Case 08 / Case 09 / Case 10 / Case 13
[212] Case 04 / Case 08 / Case 09
[213] A phrase in common usage that describes a sudden or unexpected loss of nerve or confidence (Monk, Kanter, Jamison, & Russell, 2020).

organisation. As described by Detective N08, this externality triggered an increase in planning activity during the crime phase:

> There was an awful lot of planning in relation to the 2013 contract and how they were going to fit that payment into there. That went on for weeks and there are hundreds of emails that relate to how they were going to do it, why they should do it and why they shouldn't do it. So yeah, there was a lot of planning into getting that into that contract.

Another externality was seen in Case 04 where the associate fraudsters AF04c and AF04d advised the principal fraudster PF04 they were no longer prepared to supply him with AMEX credit cards for his personal use. This triggered replanning to identify new opportunities to satisfy his desire for an illegal income to retain the lifestyle to which he had become accustomed.

8.1.1.2 Detection Of Crime

The second group of trigger events that had an impact on planning was the possible and actual detection of the fraud. In three cases, fraudsters were alerted to their detection before arrest.[214] In Case 04, auditors identified irregularities with the victim's finances and when it was announced that a public inquiry into the financial affairs of the organisation would be held, it not surprisingly triggered increased planning that resulted in increased activity, as Detective N04 noted: 'we discovered there was a time when that internal complaint was made, he went in and started shredding documents and evidence and all sorts of stuff, so that's not the only offence, there are all sorts of different ones'.

Immediately following the execution of search warrants in Case 08, communication increased between syndicate members who had yet to be arrested. As described by Detective N08, this period of post-arrest communication centred initially on information gathering and decision making:

[214] Case 04 / Case 08 / Case 09

But when we go in there to do the search warrants, [AF08d] on a plane still, so there is a flurry of phone calls, a flurry of emails, a flurry of text messages between [AF08c] and [AF08d] and between different board members and [AF08d] going 'What's going on, what do you know about this?' and 'blah-de-blah'. So, it worked better than we could have ever imagined, afterwards we got a lot of phone stuff, intercepts on [AF08d] during that time and that's what really cemented our brief against him. Had we not have had that, we wouldn't have got that flurry of stuff because they were a very closed book. At one point they weren't going to let us do what we needed to do, so we were going to have to rip out servers. It was just obstructive, as much as they could obstruct, they did.

Similarly, following search warrants in Case 04 there was an uptake in information sharing motivated by a need to determine what evidence police had seized. The following discussion was captured via a lawfully acquired telephone intercept:

PF04: When they came around just out of interest. Did they, did they look under the beds and everything?

AF01d: Oh [principal fraudster's name] they went through my shoe boxes they went through every single room, the kids, everything, everything, everything.

PF04: Everything even under the beds to look for anything?

AF01e: Yeah look, no, they, no, well we've got no they didn't look between them well we have ensembles; they didn't look between them, but they looked under the beds, yeah.

AF01d: But we knew there was nothing there so one of us took them downstairs because all the BAS [business activity statement] files are there and they took all, I mean they took all the health standards, they took all, all the old ones.

AF01e: All our archives.

AF01d: They took everything. They took everything, but there was nothing in there.[215]

The nature of these conversations changed throughout the police investigation from information sharing to the offering of advice, counter-surveillance techniques and the destruction of evidence. The following discussion was captured via a lawfully acquired telephone intercept:

PF04: …the other thing we did that I can tell you, a little secret of mine, we had … um you don't, you rip them into sizes that are fairly … you then put … I then put … inside the sink alfoil … and I had a fire in there in the house.

AF01d: We had one too but that was…

PF04: Right and I just took about half an hour. So, I wouldn't have a lot of smoke I just had flame. The reason you put the sink alfoil is because the sink gets filthy.

AF01e: Um.

PF04: And I just sat there, and it took me about … and I had. I burnt candles in the house and bloody everything to give the house a lovely smell and whatever. One Sunday morning when the kids were all out so I … took the opportunity a lot. And we were running around the house trying to find everything and we'd been through everything about 16 times. Every time you think I've done it; I would go and have another look. And if you want to do that process [name of AF1c] just stand there light the fire. If you've got a smoke alarm take the bloody battery out or you'll … um and just sit there and do it and just cause, if you get a nice little flame going you don't get any smoke. Let it all settle and then put it in a garbage bag and into the bin.[216]

[215] Case 04 – LD Transcript – Café
[216] ibid

8.1.2 Temporal Planning Phases

As previously discussed, frauds are not single events at a distinct point in time; instead, they are made up of a series of micro events over time.[217] According to Allen's (2011, p. 31) time allocation model of criminal planning, the total time a criminal allocates to fraud can be summed up as *tp* + *tm* = *ti*, where *tp* represents the time allocated to planning; *tm* represents the time allocated to committing the crime and leaving the scene; and *ti* represents the total time allocated to fraud. However, the restricted focus of *tm* on committing the fraud and leaving the scene disregards the amount of time some fraudsters, particularly insiders, allocate to post-crime activities. Indeed Allen (2011, p. 31) noted 'given the present focus on the offender's pre-crime or planning actions, we will not consider the offender's post-crime actions'. Ignoring the post-crime activities of criminals in this way overlooks the fact that in some cases, particularly those where the principal fraudsters are insiders, observers are likely to see greater levels of planning during the post-crime phase than in pre-crime phases.

The insider data in this study reveal that in all but one case (Case 13), less planning occurred during the pre-crime phases than during the fraud and post-crime phases, which partially contradicts Allen (2011).[218] However, as Allen's study focussed on robbery, burglary and other crimes rather than fraud, such comparisons are less valid as robbers and burglars are less likely to be insiders and do not need to distance themselves from the crime.

8.1.2.1 Pre-crime Phase

Unsurprisingly, analysis of the data identified an absence of pre-intent planning (see Table 14). However, pre-crime planning was identified, albeit at a lower rate than post-crime planning, as addressed later in this section. This supports the commonly held notion that most insider frauds are opportunistic rather than pre-planned (Australian Government, 2016;

[217] 'Crimes are events with a specific location in place and time. But the crime event itself is only one among many events which occur within the crime-commission process' (Cornish, 1994, p. 155).
[218] Case 04 / Case 08 / Case 09 / Case 10

Secchi, 2011). Despite this, analysis of Cases 04 and 13 identified periods of pre-crime planning with instances of collaborative planning, trial runs and preparatory actions, all focussed on ensuring the fraud was successful. Associate fraudster AF04a in the theft by a union employee case described an instance when PF04 sought to hide re-election spending by using credit cards provided by suppliers:

> I remember this meeting specifically because it was about [the principal fraudster] trying to obtain credit cards from [AF04c and AF04d]. I was one of the people who would receive a credit card if this took place. I recall during the meeting [PF04] told [AF04c and AF04d] that he wanted them to supply him with AMEX credit cards. At first, he asked them if they wanted to get an AMEX credit card. He said something like, 'How do you feel about getting an American Express Credit Card?' … they responded by indicating they already had an AMEX account and did not need any more credit cards. He then explained the situation which arose during the 1995 election and that this was why he was marking the request for credit cards. By obtaining credit cards from the [AF04c/AF04d] it would stop anyone having access to this type of information.[219]

8.1.2.2 Crime Phase

Across the insider cases, there was an increase in the levels of planning as soon as the frauds commenced. One reason for this is that all five cases were described as ongoing, rather than one-off events. This is significant as once the opportunity had arisen, each fraud required ongoing reactive planning to sustain it, whereas one-off crimes were likely to see a decrease in activity levels.

Both the extent and timing of planning varied across the cases. In Case 13, while PF13 and AF13 undertook extensive planning during the pre-crime phase, the extent of their

[219] Case 04-Statement-AF04a

crime phase planning was kept to a minimum. This was because of the level of planning they engaged in during the pre-crime phase. However, they had also agreed to sever overt communication ties 1 month before their offending commenced. This, they decided, would make it more difficult for police to make a connection between them, as Detective N13 noted:

> Even then they wouldn't contact each other, they still had their own personal phones and that was one of the hardest things to reconcile before we knew about the burn phones obviously is that they just stopped communicating with each other about 1 month before the first criminal trade started.

The fraudsters left messages on burn phones where they exchanged information, discussed new information and made plans as necessary; however, as noted earlier it was this process that led to their detection after AF13 left his burn phone at home when travelling to see PF13, forcing him to use his personal mobile phone to contact his associate and enabling police to connect the pair.[220] Limited crime phase planning was also evident in Case 04 where, other than pre-crime planning, the fraudsters undertook little to no additional planning during the crime phase. In Case 10, the planning exhibited by the principal fraudster was continuous across the fraud event timeline. The principal fraudster, faced with increasing demands from other criminals who were defrauding him, needed to continually source additional streams of investment. This suggests that while there was evidence of crime phase planning across all the insider cases analysed, both the timing and manner of that planning varied. As Detective N10 noted:

> he had to know what lies he had told everybody and I guess ultimately that became too much for him, he would have been that stressed with the different versions that he had maintained and this was even substantiated by the ladies we had spoken to by his

[220] Burner phones are used in counterintelligence, journalism, and crime. They are new, 'clean' phones used only to call and receive calls. The user does not enter any personal details on them, not access any accounts. Once finished burner phones are usually discarded and destroyed (Bradley, 2021).

office, ‘you know we often heard him’, ‘you know he would pick up the phone and answer with one and then see one ringing and not answer it and we often heard him saying things to clients, “oh you know it’s not here yet, it’s not there yet”, different excuses’. The amount of management of information he would have to be involved in, just in his own head would have been enormous.

8.1.2.3 Post-crime Phase

The data reveal that post-crime planning was more frequent in insider cases despite Detective N13 noting, ‘[i]n terms of methodologies that are being used, counter-surveillance or use of covert communications or those sorts of things, I don’t think it’s overly common’. Criminal countermeasures were seen in three cases.[221] Therefore, post-crime planning was more common than not in these cases. For the two insider cases where there was no post-crime planning, this was explained by the arrest of the fraudsters without warning;[222] in the remaining three cases the fraudsters were tipped off before their arrest or communicated with one another following their arrest.[223] This allowed them to undertake post-crime activities to reduce their chances of detection or prosecution. Such findings suggest post-crime planning should be considered in the application of the time allocation model of criminal planning to fraudsters’ activities (Allen, 2011, p. 31). The following discussion, captured after the commencement of a police investigation, was captured via a lawfully acquired telephone intercept:

AF04a: I’m in a mess, police have gone through my bank accounts and looked at all my payments, what am I going to say?

PF04: Tell them that [AF04e] gave you the money.

AF04a: Why would he do that?

[221] Case 04 / Case 08 / Case 09
[222] Case 10 / Case 13
[223] Case 04 / Case 08 / Case 09

PF04: Say that he was doing good business and just wanted to give it to you as he was a good friend. Tell [AF04e] not to say the invoices were marked up. He was a good friend and wanted to give you the money.

AF04a: Why would I give you the money?

PF04: Say [AF04e] told you to give me money too.[224]

8.1.3 Criminal Tradecraft

Analysis of the insider data identified the production of different planned outputs. This included the behaviours already addressed in Chapter 3: for instance selecting victims through specialised access positions (Felson & Boba, 2010), using particular resources (Ekblom & Tilley, 2000) and structuring criminal communication and frauds to lessen detection risk (Geis, 1970; Van Koppen & Jansen, 1998). However, as outlined in Table 14, the data analysis also produced new insights. These include delegated planning authority, rehearsals and trial runs, targeted manipulation, overriding others, counter-surveillance activities, and coaching of witnesses and co-offenders.

8.1.3.1 Delegated Planning

A feature of the insider frauds was their heightened levels of access and knowledge, or—failing sufficient expertise—their capacity to acquire access and knowledge to implement the fraud. Such autonomy provided an ideal setting for insiders to commit their crimes while planning and managing their actions, and the actions of others, to distance themselves from the crime. In most settings, insiders could plan to achieve their aims alone. However, in certain situations the principal fraudster, as an insider, needed to delegate to associates some degree of functional planning.

Having established the initial agreement for corrupt payments, PF08 continued to receive his payments with little to no oversight for how that occurred. Instead, associate

[224] Case 04 – LD Transcript – AF04a residential address

fraudsters AF08c and AF08d took responsibility for the ongoing management of the fraud—not because they received any pecuniary advantage, but because their business benefited from holding the lucrative vehicle supply contract. This fraud continued for 12 years and as each contract period came to an end, the two associates undertook additional planning to fit the corrupt payments into new contracts. Throughout this period the principal was not involved in any further planning activities. As Detective N08 observed:

> They needed to do checks on the accounts that the money was going to. There was an awful lot of planning in relation to the 2013 contract and how they were going to fit that payment into there. That went on for weeks and there are hundreds of emails which relate to how they were going to do it, why they should do it and why they shouldn't do it. So yeah, there was a lot of planning into getting that into that contract.

8.1.3.2 Rehearsals and Trial Runs

Supporting the premise that not all insider frauds are opportunistic, Case 13 provides a unique example in that PF13 and AF13 undertook trial runs and rehearsals, all aimed at refining the operationalisation of their fraud. Each fraudster would do their part of the fraud and report back to the other on the relative success or failure of their activities. As described by Detective N13, PF13 also deliberately ran up losses to make him stand out less to a keen observer:

> So, they had organised and planned to do things like have deliberate losses. So just as hard as it is to have a deliberate win on foreign exchange derivatives, it's just as hard to plan losses, but they intended to do that to again circumvent any suspicion from the brokers.

8.1.3.3 Operational Security

Analysis of the data identified the presence of OPSEC activities in three insider cases.[225] OPSEC normally describes national security and police efforts to protect critical information such as informant identities and classified materials from adversaries (McGlynn & Garner, 2019). However, the term is increasingly used to describe criminal efforts to protect their criminal enterprise from their adversaries (Jaques & Reynald, 2011; Rashid, 2016, p. 1). Driven by fear of detection, the strategies used in the current study cases varied and were seen on more than one occasion. It was not possible to determine the specific motivation for the use of concealment strategies in each case; however, as Vona (2011, p. Appendix E) contended, 'when an individual decides to commit internal fraud, how to conceal the true nature of the transaction is a critical aspect of his or her plan'. This suggests fraudsters will view any stage of their fraud, where risk increases—for example, following detection—as a necessary point at which to deploy counter-surveillance techniques.

8.1.3.3.1 Pre-crime Operational Security

Planned pre-crime concealment was observed in Case 04. Seeking to distribute their proceeds of crime the syndicate arranged to move the funds from the accounts of AF04e to those in the control of PF04 via a series of physical transactions. As noted by Detective N04:

> AF04e receives the $50k, he deposits it into a bank account. Over the next few days, he very carefully withdraws $9k, he might withdraw $27k, but does this on three separate occasions. So, in sums of $9k so as not to alert AUSTRAC. He then puts the money in a brown paper bag, and then meets up with [AF04a] at a coffee shop where he gives her a cut as well as [PF04] cut of the money.

This highlights the syndicate's awareness of control measures implemented at the retail banking level following the introduction of the *Anti-Money Laundering and Counter-*

[225] Case 04/ Case 09 / Case 13

Terrorism Financing Act 2006 (Cth). Specifically, section 43 of the act requires the reporting of threshold transactions, defined as those 'involving the transfer of physical currency, where the total amount of physical currency transferred is not less than AUD$10,000' ("Anti-Money Laundering and Counter-Terrorism Financing Act 2006," 2006). This was also observed in Case 09 where the fraudsters required reparation to be made in cash and in person rather than through the formal banking system. As noted by Detective N09:

> one guy stole from the Dandenong store down near Melbourne, on the outskirts of Melbourne, so AU$35,000, so [associate fraudster] had done all of the negotiations with him, and going to pay it back, and make him get on a plane, Tiger Airways, fly up, meet [associate fraudster 3], in the airport in the terminal, hand over the AU$35,000, and they're making him get on a plane and go back, all to avoid putting money into the financial system.

Deliberate efforts to minimise communication between syndicate members and reduce the amount of evidence police might detect were also evident. As previously highlighted, PF13 and AF13 in Case 13 limited their communication 1 month before the commencement of their fraud, which proved to be a challenging factor to reconcile for police. They used stolen identities to acquire burn phones registered in false names that were used at predetermined times. For example, the fraudsters only checked the phones once a day and when they needed to communicate, they left messages with the information request, then checked back 24 hours later. Similarly, the associate fraudster AF08d in Case 08 was highly resistant to any communication via email, as described by Detective N08:

> But we even have a series of emails where he does talk about [counter-surveillance techniques], 'I don't want this in writing anymore, it needs to all be verbal. I have never been wrong on anything before, and I won't be wrong on this one either'.

8.1.3.3.2 Post-crime Operational Security

As highlighted in the 'temporal planning phase' and 'planning trigger' sections, there was a marked increase in post-crime planning following police intervention. During this post-crime phase, an increase in planning activities occurred to keep incriminating evidence out of the hands of police officials. As noted by Detective N04:

> there was a process where he was destroying documents. There was an internal complaint before the police were involved, when the police started halfway through, we discovered there was a time when that internal complaint was made, he went in and started shredding documents and evidence.

The same offender also sought aid from an employee to destroy incriminating evidence on his laptop, as outlined in the following conversation captured on a legally intercepted surveillance device:

> PF04: Mate I've got files on my computer. I need to get rid of them. I need to make sure these files cannot be traced.
>
> OT04b: The files … were word documents of which had 'CANME' in their file names. The word 'CANME' had no meaning to me. I advised [PF04] that there is no method of securely deleting files and told him that everything could be forensically traced.
>
> PF04: Just do it.
>
> OT04b: I told [PF04] to leave this request with me. I accessed my laptop computer, I remotely accessed [PF04's] laptop through the computer network which contained the files he had shown me. I performed a move operation which transferred the files from his laptop to a USB drive … [t]his provided the physical appearance of the file being deleted and the file did not appear in [PF04's] laptop recycle bin.[226]

[226] Case 04 – Statement – OT04b

8.1.3.4 Manipulating Others

Analysis of Cases 04, 08, 09 and 10 identified periods of witness and co-offender coaching. The timing and intent of the manipulation varied with evidence of pre-crime, crime phase and post-crime efforts. An example of pre-crime manipulation is provided by Case 04. PF04 established an authoritative environment where no one was confident to challenge his actions, regardless of their nature. For example, the CFO, OT04a who worked for the principal fraudster suspected irregularities but was not sufficiently confident to challenge his boss (PF04) given his psychopathic personality, as noted in footnote 95.

Crime phase manipulation was also evident in several cases.[227] While the manipulation displayed by PF04 prevented oversight of his actions, PF09 in Case 09 set out to manipulate others to execute his crime. For example, he needed access to a procurement system that fell outside his delegated authority; so, to satisfy this need he relied on charm and charisma to effect the desired outcome. As Detective N09 noted:

> he's an ex-copper, gift of the gab, plenty of hair gel, smooth with the ladies, he had everyone eating out of the palm of his hand. He and his boss, both ex-cops, they used that, 'we're ex-policemen, you need to trust us' line. So, they built this little thing where they were just telling lies, and no one ever latched onto what they were doing.

A further type of manipulation was evident in the post-crime phase. As previously described, AF04a sought advice from PF04 on how to answer police questions.[228] Similarly, PF09 sought to manipulate others during the post-crime phase; this time, as recorded in a legally acquired telephone intercept, he contacted a witness to ascertain whether police had

[227] Case 08 / Case 09 / Case 10

[228] An excerpt drawn from 'Case 04 – LD Transcript – AF04a residential address'. [AF04a] 'I'm in a mess, police have gone through my bank accounts and looked at all my payments, what am I going to say?' [PF04] 'Tell them that [AF04e] gave you the money'.

been in touch with them. Where they hadn't, he began coaching them to help divert potential attention away from his frauds:

> PF09: If they [police] ask you anything about me just say no knowledge about me, just say you bought them [iPhones] from the markets, something like that …
>
> OT09: Where are we saying we got them from?
>
> PF09: Mate just say you got them from the markets, you know the trash and treasure ones, you know the ones everyone um … whatever … trash and treasure markets mate. Like I said they've been recovered, so I said, I didn't steal anything mate … so just deny any knowledge about me. Just say they came from the trash and treasure market, one of those down there near your place.[229]

8.2 Planning and the Outsider

Although insiders benefit from their access, outsiders do not. Instead, bereft of unchallenged access and up-to-date knowledge, outsiders devise strategies to compensate for their access and information deficiencies. As in the previous section, the outsider data are separated into three broad groupings: planning triggers, temporal planning phases and planning outputs. The first sub-section examines the temporal spread of planning along a fraud event timeline. The second explores the factors that triggered sudden increases in planning, and the third sub-section examines the manifestation of criminal planning in frauds, which historically has not considered frauds committed by outsiders.

8.2.1 Planning Triggers

As in the insider cases, the planning of frauds by outsiders was influenced by the presence or absence of access to, and knowledge of, organisational systems. The analysis of the outsider data revealed a greater range of planning triggers that brought on periods of increased planning relative to the insider cases.

[229] Case 09 Facts Sheet Participant PF09

8.2.1.1 Crime Initiation Planning

The most common phase in which planning occurred was the pre-crime phase with evidence of extensive planning undertaken by the principal fraudsters and their associates across all eight cases. As Detective 02 noted:

> Just, for example, this guy recorded his own computer and didn't realise. It [recorded] what he did for the day, he sat down and talked about fraud, went out, did what he had to do in the furtherance of fraud and then came back and did more fraud and this guy, the cybercriminals, usually sleep weird hours, they are up at 3 am researching away and sleeping. When the banks are open, they are up again, getting ready for implementation, if it is implementation day, they are up doing all that stuff.[230]

The planning in this early phase was attributed to the need to overcome access and information deficiencies. However, the exact process adopted in each case varied. In technology-enabled cases, the pre-crime planning involved sourcing compromised or uncompromised POS devices and hacking them to affect the card skimming frauds. The latter approach involved importing or stealing devices in what was labelled 'cutting crimes'. Cutting crimes required the thief to enter a store that used a particular model POS device, reach over the counter, grab it and, with a pair of wire cutters, cut the electric cables before running from the store. This initiating theft itself required planning, which was part of the larger planning event contributing to the main fraud. As Detective N05 remarked:

> They are having to firstly obtain the skimming devices; we are aware that they can obtain an EFTPOS terminal from predominately two overseas places. Australia didn't deal in wireless EFTPOS terminals, if you want one you go to the manufacturer. Overseas that's not the case so they can take second-hand EFTPOS terminals and deal with them. So, we are aware that they bought the terminals into Australia for $900

[230] Case 02

each. Through software manipulation, they can turn that device into a skimming device.

Other instances of sourcing overseas assistance in the pre-crime phase were observed in Cases 02, 06 and 12. In each case, international connections provided resources in the form of technical guidance, skimmed card data or, as in Case 12, specific criminal guidance from a facilitator. In other instances, the fraudsters allocated time during the pre-crime phase to recruit mules and runners to undertake the riskiest roles including withdrawing cash from ATMs in exchange for a minor percentage of the criminal profits (Broadhurst et al., 2014, p. 7; Chabinsky, 2010). As Detective N02 noted:

> While that is going on, they are looking for a potential person (mule) to impersonate that person (victim), there's two different MOs [modus operandi] that this group was using, the first was to get someone to impersonate the victim and transfer money out, take the money out as cash. The second option would be to actually get a mule in, a low-level person using their own details which they don't care about if they get arrested, someone will basically agree to allow their bank account to be used to obtain funds in there which they would have.

8.2.1.2 External Factors

External factors were identified as another predictor of increased offender planning. The nature of the external factors varied and was largely dependent on the duration and type of fraud. For instance, in Case 02, the account takeover fraud, increases in planning-related activities were frequently linked to instances where, having purchased skimmed card data from carding portals and finding the data were obsolete, the fraudsters had to begin again to identify new victims.

In a similar manner to Case 03, Case 06, the card skimming fraud targeting service stations, provides another example of how the implementation of fraud prevention controls

triggered periods of stigmergic planning (Nieto-Gomez, 2016). This syndicate operated their card skimming between 2007 and 2011, with early iterations of the fraud being run in Canada and the United Kingdom. By 2009 the syndicate was fully operational in Australia. Over the 5 years it operated, POS technologies went through a series of model updates, introducing new internal technologies and security features. These technologically generated extraneous factors had an impact on the crimes and necessitated periodical learning of complex code updates to ensure the ongoing viability of the skimming operation. This forced the syndicate to commit time and resources to re-imagining how they would implement the new technologies more efficiently. As Detective N06 remarked:

> you've got your device, which captures the card data with an overhead pin-hole camera, very inefficient, 50:50 chance of getting the pins matching up with the card numbers. As [the technologies] evolved you then had a pin-pad underlay that was wired into the card data, and so the two pieces of information should match up. But they are still not at 100% accurate, but more efficient than the pin-hole camera. Obviously, the GSM transmission and the Bluetooth transmission were very efficient because that was real time. Basically, they [customer] go pay for your fuel, by the time they walk in, pay for it, by the time they get back to the car, drive home they've [fraudsters] already got their card data their PIN number, encoder, another card and withdrawing funds from their account before they get home.

8.2.1.3 Detection Of Crime

The single most frequently cited cause of increases in planning was the threat posed by potential or actual detection of the frauds. In Case 01, the procurement fraud within a financial institution, the trigger was the emergence of an internal whistle blower (Chaikin, 2018). The whistle blower was responsible for ensuring software contracts entered into by the victim organisation were 'financially viable, legally sustainable, represented an acceptable

level of risk, compliant with legislation and met all of the [victim organisations] policies and procedures'.[231] The whistle blower became increasingly concerned about serious shortcomings and irregularities with the procurement deal being championed by AF01a and AF01b, and feared their inappropriately close relationship with PF01's business had compromised their integrity. However, not long before the conclusion of the deal, to which the whistle blower continued to object, an internal restructure was announced in his direct work area that ended his service with the victim company.[232]

AF01a and AF01b responded to this unwanted attention via normal operational channels; they relied on their seniority in the organisation to override the concerns raised by the whistle blower and convinced senior management of the viability of their deal. Ultimately, AF01a triggered the internal restructuring process and the whistle blower was the only staff member who did not resecure their old position at the first interview. AF01a re-interviewed the whistle blower and made the final decision to terminate his employment. This was conveyed to the principal fraudster in a text message: 'Oh don't worry. He's gone'.[233]

PF05 and AF05a in Case 05, the card skimming fraud targeting taxi patrons, were forced into replanning when taxi drivers who had previously skimmed for them the debit cards of his customers was arrested. While fraudsters PF05 and AF05a were not identified, the arrest of their former associate necessitated additional planning to identify a new taxi driver willing to assist them with this fraud.[234] To achieve this aim, one syndicate member hailed a taxi ride with a driver of the same ethnicity. Once his ride was complete and he had paid his fare, he asked the driver what percentage return he received on the EFTPOS terminal that was running in his cab, to which the taxi driver replied '2%'. The fraudster offered the

[231] Case 01 Statement OT01a
[232] ibid
[233] Case 01 – Facts Sheet
[234] Case 05 – POI Transcript 1

taxi driver the potential to make a 7% return on his EFTPOS transactions.[235] Having gained the driver's attention, the fraudster over a series of further meetings convinced him to use the fraudulent device in his taxi.

In Case 07, the debt factoring fraud, an unknown event triggered an increase in planning. The fraud commenced in 2008 and relied on the lie that an organisation where associate fraudster AF07a worked was sending all its vehicle fleet exclusively to the business owned by PF07 for servicing. To deceive the victim companies who provided debt factoring services, documentation relating to outstanding debts and contracts was regularly sent by the victim organisations to associate fraudsters AF07a's organisation as per normal business practices used by debt factoring companies to confirm the projected work, as a form of fraud control before releasing funds. However, before mid-2009 something occurred at the associate fraudsters' workplace that triggered a revision of the fraud. The principal fraudster PF07 set up a false post office (PO) box with a name similar to that of the company at which AF07 worked. She then notified the victim organisations of the change in postal arrangements, giving a series of plausible justifications for doing so. While the true nature of the trigger event remains unknown, the outcome was an increased period of planning followed by a change in the fraudsters' modus operandi.

8.2.2 Temporal Planning Phases

A common feature of outsiders in the cases in this study was their limited opportunity to commit offences against organisational systems and an absence of legitimate access pathways and up-to-date systems knowledge (Walton, 2006). Therefore, for the motivated fraudster, planning was essential in overcoming barriers to criminal success. This suggests that planning was likely to occur earlier in outsider frauds than in insider frauds.

[235] Case 05 – POI Transcript 1

8.2.2.1 Pre-crime Phase

There was no evidence of planning occurring before the formation of criminal intent, which was not unexpected (see Table 15). However, once intent formed, planning was evident in all eight outsider cases. While planning varied across the outsider dataset, all detectives noted the importance of planning to the ultimate success of the frauds. As Detective N05 remarked, 'There's no opportunity in this mate, it's all planned'.[236]

Case 07, the debt factoring fraud, was described by Detective N07 as opportunistic; almost spur of the moment. However, the actual process of debt factoring required both the falsification of business records and the creation of fraudulent documents. Coupled with this, PF07 had to deceive debt factoring companies into believing she had a high volume of work to justify the size of the factoring contracts. Knowing the factoring companies would verify the scale of the work contracts she co-opted the associate fraudster AF07a, a manager at a large organisation with a large vehicle fleet, to troubleshoot verification requests sent in by victim organisations, and to set up a false PO box address with a name similar to that of the associate fraudster's employers. This allowed the principal fraudster PF07 to screen all communication requests between the victim organisations and the company that might have been able to identify her factoring submissions as fraudulent. Therefore, although Detective N07 considered that this case was opportunistic and slowly evolved into a planned fraud, a level of planning was evident during the pre-crime phase.

Similarly, Detective N01 contended that Case 01, the procurement fraud in a financial institution, was largely opportunistic, requiring little in the way of upfront planning. However, an analysis of the data revealed PF01 engaged in detailed planning during the pre-crime phase. While the principal fraudster's specific planning actions at this phase of the fraud were not known, what was apparent was the intent of those decisions and actions. In

[236] Case 05 – Detective N05 Transcript

this case, police ascertained PF01, a citizen of the United States of America, had a history of embedding sympathetic associates in organisations, enabling him to leverage those connections to his financial advantage (see footnote 200).

Several cases reveal extensive levels of planning in the pre-crime phase.[237] For example, in Case 12, the superannuation fraud, the range of pre-crime planning was significant and included a meeting in Amsterdam between principal fraudsters PF12a, AF12k and the criminal facilitator OT12, who police believe was behind this syndicate's crime.[238] It involved the recruitment and subversion of upwards of 11 co-conspirators who ran specific tasks on the day of the fraud, including hacking telecommunication exchanges, authorising funds transfers and laundering the funds through various international financial systems. This pre-crime phase also involved specific instances of upskilling: the telecommunications technician learned the location of specific communication lines that operated securely between the two victim organisations, culminating in a trial run to confirm everything was in place.

Both Cases 05 and 06 also show levels of pre-crime planning. Both involved debit and credit card skimming frauds leading to account takeovers. Both frauds involved the importation of wireless POS devices and subsequent compromise. Compromising a POS device involves manipulating the internal coding so Track 1 and Track 2 data are captured along with the PIN.[239] Fraudsters also had to ensure printed receipts matched ones from an uncompromised device, and to identify and compromise business locations to install the compromised devices. In Case 05, the card skimming fraud targeting taxi patrons, this was achieved by subverting taxi drivers and having them use the compromised POS devices, whereas Case 06 case involved covertly installing compromised devices in service stations.

[237] Case 01 / Case 05 / Case 06 / Case 11
[238] Case 01 Facts Sheet 1
[239] See (Gomzin, 2014)

Table 15

Outsider Planning Data

	Planning triggers			Temporal planning phases				Planning and decision-making outputs											Victim selection		
													Backstopping								
Case	Crime initiation planning	External factors	Detection of crime	Pre-intent phase	Pre-crime phase	Crime phase	Post-crime phase	Delegate planning	Associate roles critical	Rehearsal and trial runs	Manipulation of others	Concealment strategies	Virtual and physical offices	Hosted site visits	Resources	Victim selection	Managing others	OPSEC planning	Employment	Apathy & weak controls	Profitability
01	X		X		X	X	X	X	X		X	X	X		X	X		X	X		
02	X	X			X	X			X			X			X	X	X	X		X	
03	X	X	X		X	X			X		X	X	X		X	X	X	X		X	
05	X	X			X	X			X			X			X	X	X	X		X	
06	X	X			X	X			X		X	X			X	X	X	X			X
07	X		X		X	X			X			X	X	X	X	X	X	X		X	
11	X				X	X			X			X			X	X	X	X	X		
12	X		X		X		X		X	X		X	X		X	X	X	X			X

X – indicates a positive correlation between the χ-axis and the γ-axis

Finally, the syndicates that ran mortgage frauds in Cases 03 and 11 also planned extensively during the pre-crime phase. In Case 11, the land valuation mortgage fraud case, this involved purchasing 23 near-worthless undeveloped residential property blocks from far western NSW for between AU$100 and AU$10,250.[240] Syndicate members undertook significant levels of planning to fraudulently increase the on-paper value of these properties ahead of the crime.

8.2.2.2 Crime phase

Unlike the transition between the insiders' pre-crime and crime phases where there was an uptake in planning, the opposite is apparent in the outsider data. While there remained some planning in the crime phase, there was nonetheless a slight reduction in the number of cases where planning was evident. The only outsider case where no planning was evident during the crime phase was Case 12, the superannuation fraud. The reason for this absence was twofold: first this was a one-off fraud; and second, all planning had been undertaken before the event. As a one-off fraud event, the fraudsters sought only to effect one fraudulent transaction, whereas other syndicates sought to repeat their offending on an ongoing basis. One reason for this was the value of the fraud, AU$150 million. Given the high value of such a fraud, it is likely that ongoing attempts would draw unwanted attention to the fraudster's activities; whereas, other outsider frauds sought lower returns, often spread out over several frauds. From a target selection perspective, an interesting point arises as to whether a high-value fraud committed once or lower-valued frauds committed multiple times exposes fraudsters to greater levels of risk and whether such considerations are contemplated.

The procurement fraud described in Case 01 was also one-off; though, unlike the superannuation fraud, it demonstrated ongoing planning across the fraud event timeline. As corporations routinely spread oversight processes across distinct operational units, the

[240] Case 11 – Facts Sheet – PF11

associate fraudsters AF01a and AF01b were forced to progress the fraudulent purchase of software through normal operational channels where others had a degree of oversight. To overcome this, they manipulated these control processes to affect their fraud, which ultimately exposed the questionable nature of both the procurement and their behaviour to others where it fell outside the organisational norms. This exposure triggered a high degree of planning activities by the fraudsters to override questions increasingly raised by other staff as to the legitimacy of the procurement, which resulted in the firing of the whistle blower.

The remaining cases in the outsider dataset were all classified as ongoing frauds. Each demonstrated either the ongoing victimisation of a single victim[241] or the victimisation of several victims.[242] Because of the ongoing nature of these frauds, the fraudsters needed to respond to several different unfolding trigger factors, as addressed in the previous sub-section. Therefore, these cases revealed that continuing elevated levels of planning were necessary to identify potential victims or source victim locations,[243] identify mules or runners[244] and overcome internal controls regularly.[245]

8.2.2.3 Post-crime Phase

Across the outsider dataset, there was a decline in the level of planning between the crime and post-crime phases. Planning was only observed in two of eight cases.[246] The absence of post-crime planning in the remaining six cases was attributed to the arrest of the fraudsters by police. Of the remaining two cases the level of post-crime planning varied. In Case 12, the superannuation fraud, the syndicate was initially successful in transferring AU$150 million from an Australian financial services organisation. In four transactions the stolen funds were sent overseas, initially to four separate and unrelated bank accounts:

[241] Case 11
[242] Case 03 / Case 05 / Case 06 / Case 07
[243] Case 02 / Case 03 / Case 05 / Case 06
[244] Case 02 / Case 05 / Case 06
[245] Case 02 / Case 03 / Case 06
[246] Case 01 / Case 12

AU$20.6 million and AU$30.4 million to Hong Kong account, AU$26.7 million to Switzerland and AU$71. 9 million to Greece. The syndicate ultimately made a mistake with the Greek funds transfer when they included the term ‘Pty Ltd’. Rather than suspecting something was wrong with a transfer of this number of Australian dollars into an account that had never had more than 10 euros in it, the bank requested that the sending institution resend its transfer, this time without the words ‘Pty Ltd’. At the same time the account holder of the Greek account, associate fraudster AF12f, was contacted and advised of the error. He contacted the syndicate advising them of the issue, and this triggered heightened planning activity. This included AF12c, AF12b and several other syndicate members who together organised to resend the transfer request, this time using the correct account details.

In the only other outsider case where post-crime phase planning was evident, Case 01, that planning was done by AF01a and AF01b who worked for the victim organisation. Following the completion of the procurement deal, AF01a and AF01b received approximately AU$2,530,000 in corrupt payments. Their employer later commenced an investigation into their activities that caused the fraudsters to undertake further planning activities to legitimise the payments they had received. They did this by creating false consultancies and suggested they had done work for other organisations, to explain the receipt of funds.

8.2.3 Criminal Tradecraft

Analysis of the outsider data revealed diversity in the planning outputs of outsiders. As with the insider data, some of these behaviours are addressed in the literature; for example, victimisation through specialised access positions (Felson & Boba, 2010), use of selected resources (Ekblom & Tilley, 2000) and structuring of crimes to minimise the chances of detection (Geis, 1970; Van Koppen & Jansen, 1998). There were some similarities with the insider data, including the presence of delegated planning authority, associates’

roles, rehearsals and trial runs, the manipulation of others, concealment strategies and coaching of co-offenders and witnesses. In addition to these, Table 15 provides an overview of a broader range of behaviours not addressed in the literature.

8.2.3.1 Delegated Planning

As identified in the literature (Coenen, 2008; Dellaportas, 2013; Lokanan, 2015) and the insider data in this study, principal fraudsters lacking the necessary knowledge in some instances delegate planning responsibility to their subordinates. Delegation of planning was also observed in the outsider cases. In Case 01, the procurement fraud in a financial institution, PF01 relied on two subverted insiders, AF01a and AF01b, to plan the specifics of the fraud and execute it. The planning in this case was evident across the entire fraud event timeline, unlike in the other outsider cases. For example, the planning in the early phases of this fraud involved the abuse of occupational positions to mask the fraudulent procurement deal and force it through procurement processes. This involved overriding concerns raised by junior staff members, pressuring relevant departments in the organisation to expedite the internal process, and excluding internal audit functions from the process. As noted in the police statement by OT01a:

> I was aware there was a big rush on this deal being put through. The timeframes that were being proposed, considering the amount of work that needed to be done, by a lot of people, was extraordinary … what I didn't understand was why there was an extraordinary rush, to buy software from someone else, that we were already buying and already had, and it all had to be rushed through in the weeks leading up to the Christmas break.[247]

There was, however, evidence of post-crime planning. Following an internal complaint when investigators identified suspicious payments to the two associates originating

[247] Case 01 Statement – OT01a

from an overseas business controlled by the principal fraudster, the associate fraudsters AF01a and AF01b commenced planning aimed at legitimising the appearance of the payments they had received. Indeed as Detective N01 in Case 01 noted, the two associate fraudsters, among other things, built websites to support the apparent legitimacy of the lies they told investigators after they had initially been asked questions about the origins of the corrupt payments made to them. As described by Detective N01:

> But they [the associate fraudsters] set up this company after the payments were made to justify, they tried to construct this consultancy after the fact to justify the payments, but of course, it all post-dates when the crime happened, so there was this panic, and they said oh, and then 'you never declared you were working for these companies', so they said 'no', and they changed the structure of the company to turn it into a not-for-profit, that was helping poor people, getting them water, it was just bullshit.

8.2.3.2 Rehearsals and Trial Runs

As with the insider data, there was evidence in one of the outsider cases, Case 12, of pre-crime rehearsals and trial runs. The principal fraudsters in this case undertook a prolonged period of detailed planning. Although the fraud was implemented on 24 December 2003, there was evidence of planned rehearsals before this. For example, as described by Detective 12, associate fraudster AF12b visited the Telstra exchange frequently to identify the specific telephone lines that would enable the syndicate to implement its fraud:

> AF12b entered the telephone exchange on 12 December, 20 December, and 23 December. [He] had no work-related reason to enter the telephone exchange [then] and [he] accessed the exchange to make preliminary inspections of the premises and the MDF to facilitate the hacking of telephone exchange equipment and wiring on the 24th of December, the day of the crime.[248]

[248] Case 01 Facts Sheet

The syndicate had an unplanned trial run 3 months earlier that failed. Although what caused the failure is unknown, it provided the syndicate with an unanticipated learning opportunity, as would the later planned rehearsal. As detective N12 noted:

> the original plan was the October long weekend to get that extra day's buffer, but that did not work out. It makes sense because [the criminal facilitator] had left the country just before that happened, he did not want to be here when it went down, it didn't happen and then he comes back in November, meets with the [two principal fraudsters], they meet up … but then [the criminal facilitator] leaves again before the Christmas eve thing and it all went down.

8.2.3.3 Operational Security

8.2.3.3.1 Pre-crime Operational Security

OPSEC was present in all eight cases and was observed across all phases of the fraud event timeline. Analysis of the data identified a heightened level of sensitivity to risks demonstrated by syndicate members who felt their activities might be under surveillance. For example, in Cases 02, 05 and 06, syndicates selected ATMs without CCTV coverage from which to withdraw funds while also taking steps to ascertain whether police were monitoring their activities, as noted in Case 06 by Detective N06:

> they imported a specifically compromised terminal VeriFone VX670 via courier, and that was disguised in a JVC video camera box. Talking about complexity and knowledge, they set up, well it was our strong belief, they booby-trapped the package to see if it had been monitored by law enforcement, by putting a hair in a specific place in the box and a fingernail. It wasn't something you just dropped, it was, I think it was almost 5 mm long, you notice it was there and the hair was, could it have just fallen there—the likelihood, however! It looked set up, specifically and there were [intercepted] conversations which alluded to 'was it safe to open'.

Pre-crime OPSEC activities included the use of encrypted communication devices to facilitate private communication pathways. In cases where encrypted devices were not used, syndicate members either resorted to coded language (Gambetta, 2009)[249] or abandoned electronic communication altogether and instead met in person, as noted in the Case 03 telephone intercept transcripts:

> OT03d: I'll meet you in a lift well…
>
> PF03a: (Laughs)/
>
> OT03d: You hop in, I'll hop in and we'll swap documents…[250]

In Case 02, pre-crime OPSEC included the hiring of lawyers as noted by Detective N02, who contended this occurred to distance the principal fraudsters from the arrest of the lower-level syndicate members.

> our guy said all the mules seemed to be represented by the same lawyer, so they had a contingency, we believe he was offering. If the mules got arrested, 'phone this guy (lawyer) and I'll look after you, pay for the fees for you'. That obviously helped PF02a out in two ways. The mule thought 'cool I'll get my fees paid. I'll get a hotshot lawyer; I'll get the least sentence'. The boss however controlled the lawyer, he had a close relationship with him, he's paying the bills for this guy so obviously there's a suggestion he [PF02] is protecting himself through the lawyer. They all pleaded guilty and he [PF02] gets left alone.[251]

8.2.3.3.2 Crime phase Operational Security

OPSEC activities were evident during the crime phase. The following conversation between associate fraudsters AF03a and AF03c recorded on a legally acquired telephone

[249] Case 03
[250] Case 03 LD Transcript
[251] Detective N02 Transcript

intercept captured an exchange where the fraudsters began to suspect their actions were under law enforcement scrutiny:

> AF03c: And I said what time can I pick the car up and he said look, that's still in getting pre-delivered, I'm not sure what time it will be ready tomorrow, but we will give you a call when it is done.
>
> AF03a: Yeah, mate it is sus mate, I'm telling you. The questions they were fishing, I'm telling you it was sus. Very sus.
>
> AF03c: Yep. Mmm. So, she introduced herself from, as being from Toyota Finance?
>
> AF03a: And then when I said what's your number, I'll call you back, you know, or send me an email, oh no, no, just do it all through [name of Toyota Finance employee], what's [her] number, I don't know, it's on the website. I'm telling you mate.
>
> AF03c: Yeah?
>
> AF03a: Mmm.
>
> AF03c: Sounded odd.[252]

Crime phase OPSEC activities were also evident in Case 05 where syndicate members were observed taking preventative measures to ensure their fingerprints could not be detected on the card skimming devices they used, as described in the Case 05 Facts Sheet: 'Footage clearly shows PF05 putting on clear disposable gloves on his hands in preparation to handle the laptop and equipment to avoid leaving his fingerprints or forensic evidence on the laptop and associated equipment'.[253]

[252] Case 03 LD Transcript. This exchange was captured at a time when the syndicate members became increasingly concerned that delays at the vehicle finance company were an indication their illegal activities might have been detected by the finance company or the police.
[253] Case 05 Facts Sheet

8.2.3.3.3 Post-crime Operational Security

Post-crime OPSEC activities were also evident, albeit less frequent than pre-crime OPSEC activities. For instance, members of the Case 12 syndicate used coded language and hurried in-person meetings to problem solve and then direct syndicate members based internationally to act to recover from a setback and re-implement the crime. In Case 01, the activities triggered following a whistle blower report were in one part designed to destroy evidence, while also legitimising the illegal activities of the two insiders to protect themselves from a police investigation.

8.2.3.4 Associate Roles Critical

Perhaps one of the most obvious and well-supported findings that arose from the outsider data was the importance of associate fraudsters in the commission of the fraud, given that in each analysed case their involvement was deemed critical. This was driven by the principal fraudster's need, as an outsider, to overcome their access and knowledge deficiencies. The way this manifested itself differed markedly between different cases.

Case 01 saw associate fraudsters engaging in planning activities; Cases 03, 07 and 12 saw associate fraudsters backstopping the crimes; while Cases 01, 11 and 12 saw associate fraudsters implementing the frauds. In Case 12, associate fraudsters AF12a, AF12b and AF12c acted at the direction of the syndicate's principal fraudsters. The following extract was retrieved from the Case 01 Facts Sheet:

> AF12b, and AF12a entered the telephone exchange on 24 December 2003 and the following events occurred:
>
> a. AF12b tampered with telephone exchange equipment and wiring to gain unauthorised access to telecommunications service, subscribed to [a funds management organisation].

b. AF12a, using the unauthorised access provided by AF12b, sent the fraudulent fax to [the victim organisation] telecommunication service, to have it appear as an authorised fax instruction [from the fund's management organisation].
c. There were then indications that the attempt to send the fraudulent fax, using the unauthorised access provided by AF12b, had failed to send the five (5) pages.
d. AF12a and AF12b then sent the fraudulent fax successfully, from the telecommunications company fax machine, physically located next to the MDF in the telephone exchange.
e. AF12a, using the unauthorised access provided by AF12b, then sent the 1.38 pm and 1.42 pm fraudulent fax to [victim organisations] telecommunication service, to have it appear as an authorised [funds management organisation] fax instruction; and
f. AF12a then, using the unauthorised access to [funds management organisation] telecommunications service, provided by AF12b, made a telephone call to [victim organisation] employee, AF12c.[254]

Associate fraudsters were also used in three cases to withdraw the proceeds of crime from victims' accounts.[255] As discussed by Detective N02, the use of associates in these cases was thought to allow the principal fraudster to reduce their chance of detection:

> The bosses will always, from what we know from speaking to the mules who have been arrested, they tell us what their instructions were. They are told to dress nicely; they give them things to say. For example, if they are taking money out and the teller

[254] Case 12 Facts Sheet
[255] Case 02 / Case 05 / Case 06

asks them what is this for? They always have some kind of plan about what to say to the person.

8.2.3.5 Backstopping

A unique feature in the outsider data was activities described by detectives as 'backstopping'. Backstopping represents processes implemented by fraudsters to support or validate a material fact. A material fact is something significant to an individual who makes decisions based on that fact. In a fraud case, backstopping results in a victim's decision to accept a lie as true, a lie that ultimately benefits the fraudster. As noted by Detective N03:

> When it comes to organised criminal activity with fraud, a high degree of planning needs to take place. These offenders need to know the systems that will be put in place, so they can overcome due diligence. They need to be in a position to accept a spot check, to answer appropriately with the right answers at the right time so it [fraudulent instrument] doesn't get rejected or so the process isn't thwarted, and it doesn't look smelly.

Two major methods of backstopping were identified in the data, the most cited being the use of virtual and physical offices.[256] In three cases, the fraudsters submitted finance applications,[257] invoices[258] and financial instructions to victim organisations.[259] Under normal circumstances, those submissions would be subject to checks to determine whether they were legitimate. The backstopping of those included developing websites and fake income statements to support financial applications;[260] and work-orders, using official-looking letterheads;[261] and having knowledge of the correct call-back procedures.[262] As described by

[256] Case 01 / Case 03 / Case 07 / Case 12
[257] Case 03
[258] Case 07
[259] Case 12
[260] Case 03
[261] Case 07
[262] Case 12

Detective N03, this style of backstopping relied on the victim being convinced of the legitimacy of the fraudulent request made by the fraudster.[263]

> You need somebody within that milieu to be able to answer the phone after it's been what we call backstopped. So, if you work for a company then that company needs to have a website with those telephone numbers listed as the contact numbers to confirm employment. Those telephone numbers are not actual landlines that go to the person who is receiving the call, but to a virtual office. The virtual office answers the call with a particular greeting, sounding very professional and very large like a corporation to the due diligence checker and [the virtual office staff] they will leave a message on behalf of the checker to get the crook to call back. The crook calls back when they receive the SMS and they will pull out a file in front of them and say right, the bank just called the employer in respect of this mule. They also set up electronic white pages, every open-source product that is available to backstop the credibility of a purported individual is a standard mechanism and process put in place before the loan application is set.

Backstopping was also observed in Case 01, the procurement fraud in a financial institution. In this instance, the fraudsters used backstopping techniques not to facilitate their frauds but to distance themselves from the criminality of their actions. As described by Detective N01 this involved an array of activities planned to legitimise their activities after the crime was committed:

> after the fact, they constructed an entire not-for-profit company, an entire ruse to try and justify the payments and then threatened to sue [the bank]. Set up a website, did all of that to try and justify the payments that were made and then have continued to have maintained the products and services they sold to [the bank] we're wonderful.

[263] See also Foot Note 204.

An extension of this style of backstopping was seen in Case 07 where the associate fraudster AF07a facilitated site visits to his employer's workplace to convince potential victims of the legitimacy of the crime. In this case, Detective N07 noted:

> They arranged for tours of the [location], where the [principal fraudsters] would take the factoring company heads. They'd meet with [the associate fraudster], and then do a tour of the facilities. There he'd point to every truck on the lot, regardless of whether they were Caltex, Shell; a lot of the trucks weren't even theirs, they were Shell: 'Oh yeah, they're all the trucks that [the principal fraudsters company] are fixing', 'plus we've got trucks offsite at all along the Eastern Seaboard'. A couple of the victims said, 'oh can you just check these invoices to make sure they're accurate?' 'Yep, no dramas, yep'.

8.2.3.6 Resources

Crime occurs when a motivated offender has the capacity to identify and take advantage of an opportunity (Ekblom & Tilley, 2000). Based on the premise that capacity, and capability (Wolfe & Hermanson, 2004) increase with experience, coupled with the acknowledgement that frauds generally tend to exploit weaknesses in functional organisation systems built around forms and processes, it appears that capability includes the ability to create, source, manipulate and manage resources towards an intended outcome.

Given the differing array of frauds, systems and controls in the outsider data in this study, the role of resource manipulation was prominent. The sourcing, manipulation and management of resources was influenced by a range of factors, pointing to a high level of rationality. For instance, the recruitment of co-offenders is a resource because selecting the right co-offender, upskilling them and providing them with instructions are considered 'personal resources' or capabilities at the disposal of the principal criminal. This type of

resource was observed in three cases.[264] In Case 02, the account takeover fraud, Detective N02 identified that the principal fraudster would recruit mules to match the physical descriptions of victims:

> the mules can vary depending on what is needed; so for example if they want someone to pretend to be a 40-year-old male they recruit a 40-year-old male; otherwise, they just get university students to go in and open accounts and they put money in those.[265]

The principal fraudster then provided mules with instructions tailored to the unique needs of a particular fraud. An example of this was also drawn from Case 02, the account takeover fraud, as observed by Detective N02:

> The first thing the [principal fraudsters] tell them to do is dress nicely, 'you don't want to go in looking like a bum' as they would obviously get a bit sus. So, the way they [mules] present themselves is … the bank's system is to use people's intuition to work out or identify if this guy [the mule] is the real person they are purporting to be.

The outsider data provide a range of further examples of how resources were used; for example, bringing together information sources to satisfy information demands. As discussed by Detective N02, in the account takeover cases the fraudsters sourced information on victims:

> the starting point is they've got some information, name, date of birth address, all that kind of stuff phone number, that's a good starting point. Anything else they are missing, such as the signature, they'll do other checks through mortgage, the land titles office, when you sign … your signature is there, they have done ASIC

[264] Case 02 / Case 03 / Case 05
[265] See Broadhurst et al. (2014) and Chabinsky (2010) for descriptions of mules in criminal syndicates.

> [Australian Securities and Investments Commission] checks, they use dodgy credit cards, so it doesn't cost them; they obtain the signatures and build up a profile.

Technical resources were also deployed; for example, in card skimming cases the syndicates either purchased or stole suitable POS devices.[266] Indeed, Detective N06 noted:

> The vehicle to carry out the crime is incredibly complex in that a POS needs to be manipulated to capture the data in a fashion that is not detected by the LEA [Law enforcement authority] or the public or the acquirer while avoiding the anti-tamper mechanisms in place on the terminals. Furthermore, down to matching card data. So that incorporates the manipulation then you've got the setting in place of the terminal or the [compromised POS]. The period of use is the risk of detection, and then the removal of the [compromised POS], downloading of the product, and then the encoding of the fraudulent cards to obtain the financial advantage. So, the encoding of the PVC cards and the like. So that's one very complex aspect. Then it goes, the crime type evolves so the complexity evolves from having foreign electronic components covertly installed in the terminal, through to the terminal being manipulated through software only, where there are no physical 'tells' that a terminal has been compromised. And so, you are getting to the mechanics of how terminals operate, how does someone, an offender, how does an offender gain the knowledge that this can be done, and then how do they gain the knowledge of how to do it, ensuring they've got the, not only the knowledge, but the resources to do it?

8.2.3.7 Victim Selection

Analysis of the outsider data provided insights into why the fraudsters selected specific victims, with ease of access gained via employment as the main reason. In two of

[266] Case 05 / Case 06

those cases, that access was through associate fraudsters' employment,[267] while in the other case, the selection was based on ongoing daily interactions between the victim and the fraudster.

The apathy of the organisation and insufficient controls were identified as major factors influencing the fraudsters' selection in four cases.[268] As suggested by one detective, large institutions are less likely to notice small losses, and where identified they are more likely to write off the loss.[269] The fraudsters in Case 05 approached this from a different perspective. As Detective N05 noted:

> the principal [PF05] had his people target businessmen and drunks. A businessman has a corporate credit card and doesn't generally check the statement until the end of the month, so [PF05] 1 month of using the credit card. Drunks don't see you skimming their card, they're either falling asleep in your cab or being sick. That is the specification that the head of the syndicate gave to his underlings.

A final criterion, victim selection, related to the potential net gain particular victims would yield. As described by Detective N06, the fraudsters in Case 06, the card skimming case at service stations, demonstrated highly rational planning when selecting offence locations:

> They conducted a feasibility study on the location, terminals are normally compromised and put into place for about 2 weeks, 2–4 weeks, on average [fraudsters] like 400 cards a day utilised at the merchant location, for a 2–4-week period. Normally 2 weeks because they get nervous as they want to download the information before it's found out.

[267] Case 01 / Case 11
[268] Case 02 / Case 03 / Case 05 / Case 07
[269] Case 02

8.3 Summary

The analysis presented in this chapter suggests that rather than insiders simply relying on their own access, they undertake greater levels of planning than previously suggested (Australian Government, 2016). This undermines the common perception of insiders as merely opportunistic actors by revealing they are more closely aligned to outsiders than previously thought. Planning generally occurred for one of three reasons, the first of which was crime initiation planning, which occurred during the pre-crime phase (Allen, 2011). The second planning trigger was the presence of extraneous factors' those that negatively impact the likelihood of the success of the fraud and were largely unanticipated. This includes technological changes, changes in internal policies, the end of contracts and the ongoing nature of the crime. The final planning trigger, the detection of crime, triggered the highest levels of planning-related activity across all fraud event timelines.

The temporal distribution of planning differed between the insider and outsider cases. Insiders were more likely to be observed planning during the crime and post-crime phases, rather than in the pre-intent and pre-crime phases; while outsiders were more likely to demonstrate planning behaviours during the pre-crime phase, with little to no evidence of post-crime planning. Applying this to the time allocation model of criminal planning (Allen, 2011) suggests an insider's peak activity periods are located in the latter part of their fraud event timeline and an outsider's peak activity periods are located in the earlier stages of their fraud event timeline. This has implications for where potential evidence might be located. This chapter also described a number of planning and decision-making outputs that were evident across both datasets. These unique outputs include delegating planning responsibilities to subordinates, rehearsals and trial runs, backstopping, victim selection techniques, witness and co-offender coaching and OPSEC considerations, all aimed at shielding the principal fraudsters from scrutiny.

Chapter 9: Discussion

This thesis aimed to analyse the influence of a fraudster's proximity to a target financial system on the tradecraft they employed. It approached this analysis from the perspective of a process analysis with three distinct foci: specifically, how fraudsters gain access to their victims; how they acquire the necessary knowledge to commit their crimes; and how they plan and implement their frauds. The tenets underlying of this study were:

1. Frauds cannot be effectively controlled unless their underlying mechanisms are understood.
2. Despite legal definitions, all frauds are unique to the setting in which they are committed.
3. Each setting provides a unique set of variables.
4. Proximity to the financial system is the principal variable that shapes a fraudster's tradecraft.

The use of the ALPi model in this thesis has provided a detailed picture of the differences between insider and outsider approaches to access, learning and planning.[270] Building on the four points above, this thesis set out to answer the following research questions:

1. To what extent are differences in the selection and deployment of tradecraft influenced by whether a fraudster is an insider or an outsider to the target financial system?
    a. How does access to financial systems differ between insider and outsider cases?
    b. How do learning and knowledge acquisition differ between insider and outsider cases?
    c. How do planning and preparation differ between insider and outsider cases?

[270] See (Allan, 2018)

Chapter 5 presented a synopsis of the 13 criminal investigations at the centre of this thesis. Chapters 6, 7 and 8 presented the findings of this thesis. Drawing on these chapters, the current chapter presents a synthesis and discussion of the findings, highlighting pertinent new information that can inform the development of more efficient financial crime control mechanisms.

9.1 ALPi Model

The purpose of this section is to draw on the findings presented in Chapters 6, 7 and 8 to reframe the ALPi Model. The addition of temporal activity phases and a task frequency allowed the ALPi Model to provide a more nuanced approach to the examination of fraudsters' tradecraft practices. In this way the model provides a method of differentiating between the offending patterns of insiders and outsiders, which facilitates a more precise understanding of how fraudsters approach the commission of their crimes. Finally, this section uses the ALPi Model to refine the time allocation model of criminal planning[271] and the fraud triangle.[272]

9.1.1 Temporal Variation in the Implementation of Tradecraft

The ALPi Model was initially conceived as 'a framework to elicit greater detail around how criminals approach their crimes' and was viewed only as a synthesis of access, learning, planning and implementation (Allan, 2018, p. 38). According to this initial version of the model, the insiders in the cases in this study gained access to victim organisations via legitimate workplace employment, and built knowledge, skills and expertise through work-based experience and on-the-job training (see Figure 8). This provided insiders with knowledge of how to target financial systems functions and their controls. Having formed criminal intent, they then planned and prepared their crimes before implementation. It is

[271] (Allen, 2011)
[272] (Kassem & Higson, 2012; Wells, 1997)

important to note that the level of planning that occurred between the formation of criminal intent and the implementation of the fraud varied among cases, with some showing only cursory consideration and others being complex and meticulously planned.[273] Finally, in the event of workplace or police detection, insiders displayed periods of intense learning and planning to distance themselves from the crime, to shift responsibility or deny the illegal nature of their act.[274]

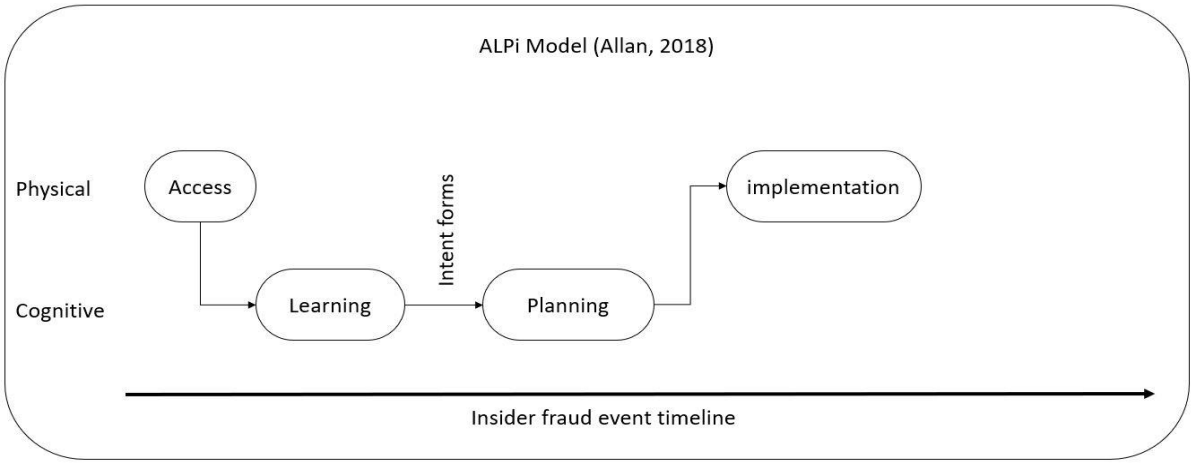


Figure 8. Simplified insider model (2018)

Outsiders, because of their lack of access via occupational positions, demonstrated a different temporal sequence to their crimes. Rather than access, learn, plan and implement, outsiders instead transitioned through a repetitive cycle of learning and planning until they had acquired the knowledge and skills necessary for them to understand the workings of the target financial system, and how it responded to illicit incursions. Following this, outsiders gained access to the target financial system to implement their crimes (see Figure 9).

[273] The variety in the level of pre-crime planning was similar to that which burglars demonstrated in the study by Bennett and Wright (1984).
[274] Blaming others and denying the victimisation of others was especially prevalent in cases where an insider was involved.

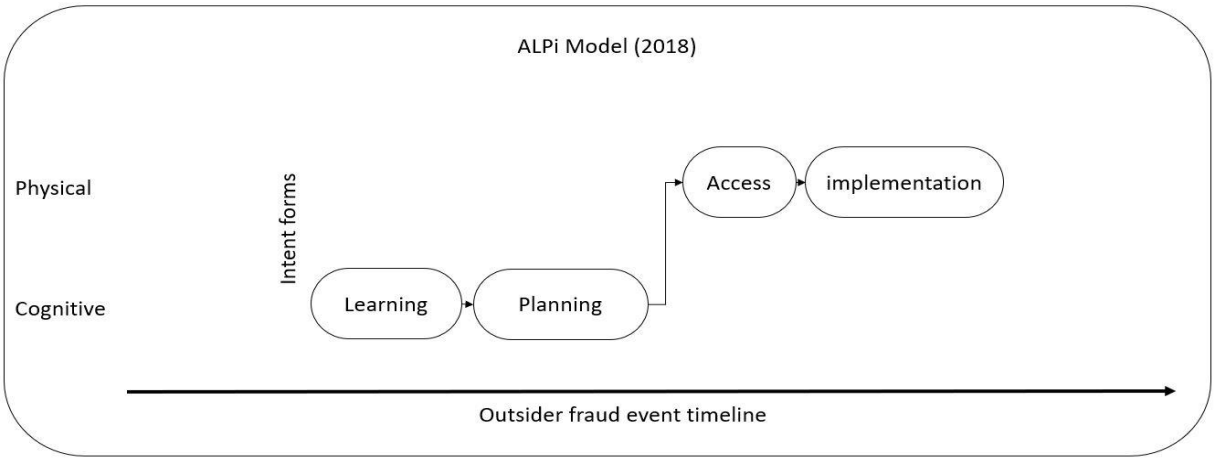


Figure 9. Simplified outsider model (2018)

Although the initial version of the ALPi Model synthesised access, learning, planning and implementation, the identification of the temporal activity phases of pre-intent, pre-crime, crime phase and post-crime phases of offending has led to its refinement. Figures 10 and 11 reflect the revised version of the ALPi Model drawing from the case data. This provides a more detailed overview of how the offending processes of insiders and outsiders differs. Key changes to the ALPi Model include replacing 'physical' and 'cognitive' processes in the vertical direction with 'task frequency'. This provides a way of visualising the finding that fraudsters display higher levels of task frequency at certain points along the fraud event timeline than others. Therefore, the higher a task is positioned inside a temporal activity phase, the greater the level of temporal activities undertaken.[275] The implication of this is that evidence, or activity traces associated with criminal intent, may be more apparent in some phases than others.

[275] As no two crimes are the same, quantifying task frequency cannot be achieved via the specification of a set number of events per temporal activity space. Rather, it is a subjective assessment based on the activities of the syndicate across the entire length of the fraud event timeline.

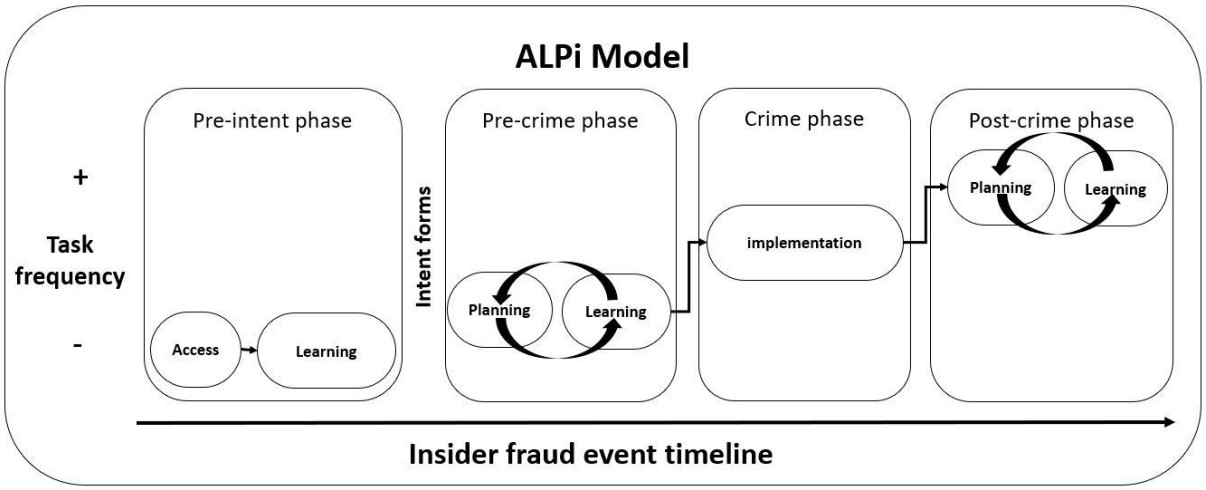


Figure 10. Revised insider ALPi Model

When considering the insider cases, it was evident that task frequency levels in the pre-intent temporal activity phase were consistently low across the insider and outsider cases (see Figures 10 and 11). This, it is theorised, was because activities leading up to the formation of criminal intent were undertaken in the absence of any pressure linked to criminal events. In the case of insiders, they learned how the financial system operated following the commencement of their employment. Meanwhile, outsiders were potentially drawing on experiential learning opportunities built around previous employment opportunities, as well as previous criminal experiences.

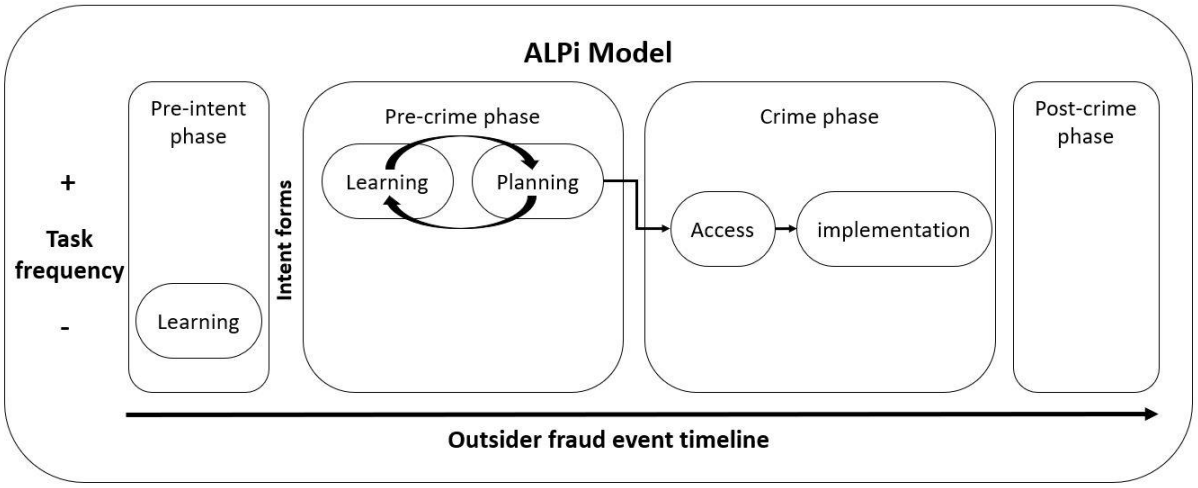


Figure 11. Revised outsider ALPi Model

After criminal intent was formed, the task frequency of both insiders and outsiders increased. However, outsiders typically engaged in more pre-crime activities than did insiders, because of their inherent disadvantage compared with insiders concerning knowledge and access. Therefore, as shown in Figure 11, their learning and planning-related activities were generally more frequent than those observed in insider cases (see Figure 10). The significance of this increase in activity is that while insiders demonstrated some increase in their pre-crime activities, outsiders' activity increases were substantially greater. Indeed, this was the point along the fraud event timeline sequence where outsiders were at their busiest, as noted by Detective N02:

> they usually sleep weird hours, they are up at 3 am, researching away. Then sleeping, then when the banks are open, they are up again, getting ready for implementation, if it is implementation day, they are up doing all that stuff.

Analysis of the data revealed that in the crime phase, insiders were busier than they had been in the pre-crime phase, whereas outsiders undertook fewer tasks than they had in the pre-crime phase. The data suggest that insiders spent a significant period confirming the successful implementation of their crime, whereas outsiders tended to step back from their crimes and act only where explicitly needed. The data suggest that the reason for this difference was twofold. First, insiders did less planning than outsiders in the pre-crime phase, which meant there were more tasks to be completed on the day of the crime. Second, insiders were also less experienced criminally than outsiders and therefore were less certain about the likely success of their criminal enterprise, as highlighted by frequent interactions between co-offenders to check the crime was going to plan.[276]

[276] This supports the premises originally made by Sutherland (1947) that individuals that have interacted with law enforcement in the past are more criminally mature than those who had not. In the case of this thesis, six of 13 cases revealed the presence of syndicate members with previous criminal convictions.

However, the single biggest point of differentiation between the two groups occurred during the post-crime phase. Insiders, those who had not been arrested, tended to be the busiest during this phase of the crime event timeline. The insider data provide extensive evidence of syndicate members probing each other for information on how the crime had gone; whether they had met any resistance; and, where there was the chance of detection, what if anything they had said to police or others, and what had been asked of them. In contrast, outsiders' actions were conspicuous by their absence during the post-crime phase, with little to no activity evident across the entire dataset. Overall, insiders were quieter at the commencement of their fraud event timeline and tended to get busier towards the end, whereas outsiders tended to start out being more busy and become quieter towards the end of their event timeline.

The addition of the temporal activity phases to the ALPi Model has several advantages for an analysis of fraudsters' tradecraft practices. First, it overcomes the confusion created by the suggestion that access, learning and planning are linear stages of a crime (Allan, 2018, p. 38), rather than broader tradecraft classifications undertaken by fraudsters at distinct points in time. Second, it establishes the existence of discrete activity phases. This assists in conceptualising the presence of distinct foci points that researchers might expect to observe along the fraud event timeline. Finally, it assists in conveying differences between similar tradecraft practices that occur at different times in the event timeline. For example, Figure 10 depicts 'learning' in three of the four temporal activities usually present, once in each of the pre-intent, pre-crime and post-crime phases. This is important because the learning undertaken during the pre-intent phase is likely to be general, restricted to understanding the legitimate workings of a victim organisation's systems, whereas, pre-crime learning, which occurs after the formation of criminal intent, is likely to be more focussed and include an emphasis on OPSEC considerations. Finally, the learning

that occurs in the post-crime phase is likely to be different again; this time the learning is likely to focus on determining the extent to which the fraudster and their crime are exposed. Consequently, the addition of temporal activity phases to the ALPi Model provides the ability to emphasise differences in the application of tradecraft practices along the entirety of the fraud event timeline.

9.1.2 Revised Time Allocation Model of Criminal Planning

As demonstrated in the previous section, insiders often undertake long periods of post-crime learning and planning with the intention of either distancing themselves from the crime, shifting responsibility to another or denying the illegal nature of their actions.[277] This finding provided the opportunity to update the time allocation model of criminal planning (Allen, 2011). As noted in Chapter 8, Allen (2011) contended that criminal planning could be expressed mathematically as the sum of $tp + tm = ti$, where *tp* refers to the time allocated to planning, *tm* refers to the time it takes to commit the crime and leave the scene, and *ti* is the total of all time allocated to the crime. However, for the reasons outlined in this thesis, this model fails to represent the complexity of the planning behaviours observed in the complex frauds examined in this study, especially the insider data. Therefore, the total time allocated to a fraudster's activity should be summed up as $tp + tm + tq = ti$, where *tp*, *tm* and *ti* are defined as above and the component, *tq*, represents post-crime counter-surveillance planning. Thus, when considering the temporal spread of planning along the fraud event timeline based on the frauds described in this section, the fraudsters are for the most part classified as mid-to-late event timeline planners.

[277] See (Sykes & Matza, 1957)

9.1.3 Revised Fraud Triangle

The fraud triangle, as initially proposed by Wells (1997), has traditionally been used to explain how frauds occur, but has been subject to ongoing revision since its inception.[278] In Section 3.1.2 it was argued that the fraud triangle is an inadequate description of how frauds are committed, and it was suggested that a revision of Kassem and Higson's (2012) new fraud triangle would aid such a description. The proposed revision involves a switch of capability and opportunity to reflect that an opportunity is always present under ideal conditions. The placement of the ALPi Model at this intersection provides a framework of analysis to more fully understand how a fraudster's tradecraft is deployed. Therefore, while the ALPi Model is used to map variation in the implementation of tradecraft practices, its inclusion in a revised fraud triangle provides a framework for analysis of not just how frauds occur, but also when and why (see Figure 12).

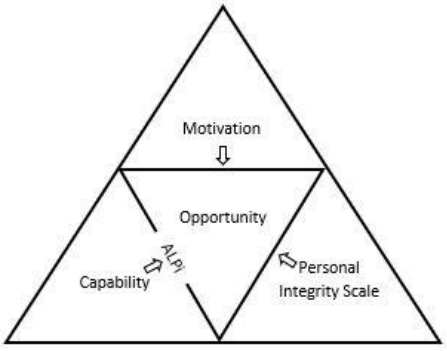


Figure 12. Revised fraud triangle

9.2 Tradecraft: Access in Financial Crimes

This section synthesises the insider and outsider data to present key findings from this thesis as they relate to how fraudsters gain access to target financial systems. The section also discusses the importance of secondary systems access and its role in facilitating financial crimes. Finally, the section proposes a revision to routine activity theory to account for an

[278] See (Albrecht, Albrecht, et al., 2006; Kassem & Higson, 2012; Wells, 1997; Wolfe & Hermanson, 2004)

oversimplification of the capable guardianship element of this theory that overlooks the agency of the offender.

9.2.1 Access via Collusive Relationships

Contrary to views that fraudsters traditionally operate alone,[279] the data analysed in this thesis show that frauds were more likely to be committed by groups than by individuals. As outlined in Tables 8 and 9, and summarised in Table 16, the data support the premise that frauds are more likely to be committed by collusion among fraudsters operating as a syndicate than by a fraudster acting alone, with evidence of collaboration in 12 of 13 cases. This was particularly evident in all eight outsider cases, reflecting the importance of criminal associates in gaining access to financial systems. Indeed, far from being individualistic, the outsider cases included the involvement of anywhere from 2 to 42 associates in any single event. Similarly, analysis of the insider data revealed that four of five cases involved associates as part of the crime, albeit with smaller syndicate sizes of two to five associates. Only 1 of 13 cases involved a single fraudster operating alone, conflicting with the view that fraudsters normally act alone.[280]

Collusion in all cases where it was evident provided outsiders with access to target financial systems or, in some instances, specific facilitation by associates to overcome access limitations.[281] However, insiders, despite their occupational positions also colluded to commit their crimes. This is evident in the crimes that could only be committed at the intersection of two separate entities. For instance, the crimes of PF13 relied heavily on early access to government employment data releases provided by AF13 in the insider trading case. This was

[279] See (Association of Certified Fraud Examiners, 2014; Biggerstaff et al., 2020; Cressey, 1950)
[280] See Free (2015) who questioned the validity of the individualising function of the Cressey's (1950) Fraud Triangle model.
[281] Helpfully, Ekblom and Tilley's (2000) seminal work identified both collaborative and facilitatory resources as a key components in a criminals arsenal.

also observed in Case 04, where an external supplier was needed to validate the passing of organisational cheques by PF04.

Table 16

Data Synthesis: Access

Criterion	Descriptor	Insiders	Outsiders
1	Collusion	Collusion evident in four of five cases	Collusion evident in all cases
2	Routine daily activities (RDA)	RDA accounts for varying degrees of access in all cases	RDA accounts for varying degrees of access four of eight cases
		Ranges from familiarity to complete access	Ranges from familiarity to complete access
3	Motivated offender	Motivation evolves	Motivation evolves
4	Suitable victim	Multiple suitability factors identified, and suitability is multi-directional	Multiple suitability factors identified, and suitability is multi-directional
5	Subversion	Pre- and post-employment subversion evident in three of five cases	Pre- and post-employment subversion evident in six of eight cases
6	Formation of intent	Access occurs before the formation of intent	Access occurs both before and after the formation of intent
7	Temporal activities/task intensity	More activity late in the crime sequence	More activity early in the crime sequence

The specific nature of a principal fraudster's occupational role was also a major factor in predicting whether they needed to collaborate with others. In Case 10, PF10, as the proprietor of a small accounting business, had oversight and control of all operational functions and thus did not need to collaborate. However, both PF04 and PF09 had quite narrow managerial roles, which meant they could not automatically access all systems in the victim organisation. Given their limited delegated authority, collaborating with others was the most efficient method of overcoming access barriers to commit their crimes. Thus, despite the influence of Cressey's (1950) modern fraud research, particularly the idea of the fraudster

working alone, this thesis found numerous examples of frauds that required the involvement of multiple actors, as increasingly observed in the fraud literature.[282]

9.2.2 Access via Routine Daily Activities

A common criminological truism that emerged from the work of Cohen and Felson (1979) is that routine daily activities bring criminals into contact with their victims (DeLiema, 2018; Williams et al., 2019). However, the findings of this thesis suggest that routine daily activities cannot consistently account for all instances where an offender and a victim come into contact. For example, while routine daily activities accounted for at least some degree of access in all five of the insider cases, it could only account for access in four of eight outsider cases. The data also suggest that rather than uniform access, routine daily activities provided anywhere from unrestricted access through to only a passing familiarity with a target financial system. Indeed, the way contact occurred also varied greatly, ranging from employment to interacting with a victim via a routine commercial interface.[283]

The data also provide evidence of differences in the way fraudsters encountered their victims. In some cases, fraudsters pursued victims because their daily activities brought them into contact with the victim;[284] for example, PF10 approached specific clients whom he believed might be open to his suggestions for a great investment, while PF07 and AF07a worked in conjunction to submit and backstop debt factoring requests to identified debt factoring companies. In other cases the fraudsters figuratively set a 'trap' and waited for victims to become ensnared (Walsh, 2014).[285] [286] For example, in Case 06 the trap, or proxy fraudster, was a compromised EFTPOS device covertly installed at a service station. Thus, it can be

[282] See (Doig & Sproat, 2020; Free, 2015; Hardy et al., 2020; Morales et al., 2014)
[283] As described in Chapter 6 a commercial interface point describes the mechanism through which an organisations financial system facilitates a legitimate connection between them and entities they normally deal with.
[284] Case 01 / Case 04 / Case 07 / Case 08 / Case 03 / Case 10 / Case 11 / Case 13
[285] Walsh (2014, p. 42) contended the selection of targets was not always a purely rational act when suggesting that in the absence of rationality military leader from Wellington to Napoleon would sometimes resort to luck and boldness when setting a trap.
[286] Case 05 / Case 06

argued that the victim's routine daily activities (going to a service station to fill a car with petrol) brought them into contact with the proxy offender, rather than the fraudster targeting the specific victim. Given the covert installation of a compromised EFTPOS device at a service station that the fraudster neither owned nor worked at, access could not be said to have arisen from routine daily activities of the fraudsters, as the data suggested these locations were scouted and selected only because they used a certain brand of POS device. Thus, it is possible to conclude that routine daily activities are multi-directional; that is, they should be viewed from the perspectives of both the victim and the offender when determining the way the offender meets their victim. This confirms that it matters not whether it is the victims' or fraudsters' routine daily activities that bring them into contact, provided of course the fraudster is ready and able to implement their crime when the opportunity arises.

9.2.2.1 Motivation

The data provided interesting insights into the evolution of fraudsters motivations. While numerous studies have examined the motivational drivers thought to lead a fraudster to crime,[287] few have paid complete attention to the way fraudsters' motivations evolve. Both the insider and outsider data in this study provide unique accounts of how such changes occurred. Money, in 9 of 13 cases, was the most common initial motivation, followed by threat of loss in 3 of 13 cases, and ego challenge in 1 of 13 cases.[288] This is similar to the findings of other studies examining fraudsters' motivations.[289] However, secondary and tertiary motivations also emerged.

In total, 9 of 13 cases involved secondary motivations. As highlighted in Tables 9 and 10, cases where money was the initial motivation also transitioned into threat of loss, sense of

[287] See (Dellaportas, 2013; Edelhertz, 1970; Goldstraw-White, 2011; Marques & Dhiman, 2018; Rustiarini, T, Nurkholis, & Andayani, 2019; Suh et al., 2020)
[288] Stotland (1977) identified seven motivational factors that influence individuals to commit crime, these include *Money*, *Threat of Loss*, *Sense of Superiority*, *Ego Challenge*, *Benefitting the Victim*, *Power*, and *Group Forces*.
[289] See (Dellaportas, 2013; Goldstraw-White, 2011; Kassem, 2018; Levi, 1999)

superiority, benefactor and addiction.[290] In the remaining 4 cases where the initial motivations were ego challenge and threat of loss, these transitioned to money.[291] Finally, 2 of 13 cases displayed tertiary motivations: in Case 01 this was an ego challenge,[292] while in Case 07 as described earlier, a form of criminal altruism or the benefactor motivation was present.

These findings provide evidence of greater levels of motivational variability by the fraudsters in the cases analysed here, which offers an opportunity for further exploration of how motivations evolve. From a practical perspective, the existence of motivational evolution suggests fraudsters' behaviours are also likely to evolve. This is evident in Case 07 where, when faced with the loss of her business, PF07 committed a small number of frauds in an act of desperation. However, as time progressed she became increasingly greedy and began to thrive on the excitement of gifting monies to local charities.

9.2.2.2 Victim Suitability

The second aspect of Cohen and Felson's (1979, p. 591) routine activity theory, victim suitability, was described as a target's value, visibility, access or inertia that have the effect of signalling a victim as a potential target. Analyses of all cases revealed that in 10 of 13, multiple factors contributed to the perceived suitability of a victim, as shown in Tables 8 and 9.

The research demonstrated that in 10 of 13 cases suitability of the target was influenced by more than one factor. Weak or non-existent controls were cited in 8 of 13 cases, followed by systems familiarity in 6 of 13; weak penalties and anonymity each featured in 3 of 13 cases and social connections in 1 of 13 cases. When compared with the

[290] Stotland (1977) identified seven motivational factors that influence individuals to commit crime, these include *Money*, *Threat of Loss*, *Sense of Superiority*, *Ego Challenge*, *Benefitting the Victim*, *Power*, and *Group Forces*.
[291] ibid
[292] ibid

original reference of value, visibility, access or inertia,[293] the data presented in Tables 8 and 9 reveal a far greater array of factors that contributed to victim selection. In particular, the suitability factors identified across the two datasets, and in the outsider cases alone, included commercial interface points and trending crime patterns, which suggests the presence of a more fluid set of situational factors that influenced victim selection, than those initially described in the literature.[294]

9.2.2.3 Capable Guardianship

Analysis of the insider and outsider data provided new insights into capable guardianship, the final component of Cohen and Felson's (1979) routine activities theory. In only 2 of 13 cases was there an absence of capable guardianship. For example, Case 08 lacked any form of oversight over the principal fraudster PF08 in his role of procurement manager, thus allowing him to structure the purchase of vehicles in a fraudulent manner. In Case 10, principal fraudster PF10 as the sole proprietor of an accounting business, was subject to no internal or external oversight. However, the remaining 11 cases show extensive evidence of seemingly adequate, or at least common modes of guardianship that ranged from multi-factor identification and SOD in regard to policies and passwords. The victim organisations in these 11 cases had multiple layers of guardianship, yet despite those protections, each organisation succumbed to fraud.

This thesis has identified that notwithstanding being compromised in the 11 cases, multi-layered guardianship mechanisms were not only present but also partially capable within the scope of their design parameters. For instance SOD, a control that some argue is an ineffective crime prevention tool,[295] was nonetheless viewed as an effective control in three

[293] See (Cohen & Felson, 1979, p. 591)
[294] ibid
[295] Barra, Savage, and Im (2020, p. 45) quantitatively examined degrees of SOD to determine the effectiveness of SOD as an effective fraud prevention control. Their study concluded that 'most degrees of separation are not effective for prevention fraud because of the increased possibilities for collusion'.

of four cases. For example, in Case 01 its presence meant that AF01a and AF01b had to engage with different control functions across their organisation to push through the procurement fraud, something PF01 wanted to avoid at all costs in pursuit of his fraud, and in these instances, this did not result in collusion. Although AF01a fired OT01a, the whistle blower, the presence of SOD ultimately led to the syndicate's activities being detected. In Case 09, the presence of SOD meant PF09 had to use a colleague's access to process procurement orders, which was not identified by internal audit until sometime after the event—again there was no collusion. Similarly, in Case 11, AF11c did not have the authority to approve a mortgage, in the absence of a physical valuation of the underlying asset; instead, this authority was delegated to an automated valuation program. Although AF11c was able to fraudulently manipulate the program, it recorded his actions, which ultimately led to the syndicate's detection. In these three cases, SOD forced the fraudster to alter their course of action in some way that ultimately led to their detection.

There was however an exception to the finding outlined in the previous paragraph. In Case 04, despite clear SOD rules in place, PF04 via sheer force of his personality overrode them for his financial advantage. Additionally, SOD remains central to the most effective financial crime prevention strategies in place today, despite its failings.[296] This raises an interesting point of contention as it relates to the reliance of routine activity theory on an absence of guardianship,[297] because in each case had the fraudsters not been equipped with the necessary resources,[298] the guardianship would arguably be capable.

[296] Guardianship overcome in the insider and outsider data, that remains part of current fraud prevention measures includes audit packages (Bradford, Henderson, Baxter, & Navarro, 2020), disclosure requirements (Seda & Tilt, 2020), checklists (Johnston & Spencer, 2011), machine learning (Nanduri, Jia, Oka, Beaver, & Liu, 2020), and multi-factor authentication (Tsai & Su, 2021).
[297] See (Cohen & Felson, 1979)
[298] See (Ekblom & Tilley, 2000)

9.2.2.4 Routine Activity Theory Revision

Based on the above discussion, this thesis suggests that routine activity theory oversimplifies the agency of successful fraudsters by downplaying the complexities of personal resources they bring to their crimes.[299] [300] It also paints the picture that controls are all or nothing; success or failure, which detracts from the reality that some fraudsters try and try again, learning each time until they successfully gain access. Indeed, while the fraudsters in these 13 cases were successful for a time, the data indicate that guardianship remained capable as those same controls continued to prevent others from accessing the target financial systems. Therefore, rather the third component being framed as an absence of capable guardianship, it should instead be considered a crime that occurs when a motivated offender meets a suitable victim and has the capability to overcome guardianship (see Figure 13).



Figure 13. Routine activity theory revision

9.2.3 Subversion

As identified by Barra et al. (2020), SOD is often sidestepped by fraudsters via the subversion of others. Considered an insult, according to Weld (2012, p. 44), being subversive is by its nature 'clandestine, something not accepted by society',[301] and the fraudsters' covert

[299] See (Cohen & Felson, 1979)
[300] See (Ekblom & Tilley, 2000)
[301] Weld (2012) examined the efforts of the Guatemalan regime under Romeo Lucas Garcia to undermine and strip political and social opponents of credibility and thus labelling them as subversive rats. Similarly, Cohen (2001, p. 84) discussed the benefit to repressive states of promoting 'the hermetic mythology about the dangers posed by subversives'.

actions in this thesis underscored an intent not to draw attention to their activities. Across the combined dataset, subversion was evident in 9 of 13 cases. The majority of these (6 of 9 cases) were identified as outsider cases, while the remaining three were insider cases where the subversion occurred in third-party organisations, not in the victim organisation.

The data drawn from both insider and outsider cases provide evidence of temporal variation in when others were subverted. Case 04, the theft by a union employee, and Case 06, the card skimming fraud targeting service stations, provide examples of pre-crime subversion. In these cases, the principal fraudster subverted another before applying for a role with the victim organisation. For example, in Case 04, PF04 subverted AF04 to his crime and then encouraged him to tender for printing contracts, which facilitated the theft of funds from the target financial system. In Case 06, an associate fraudster, AF06f(1), was recruited to the syndicate and then instructed to apply for a job at one of the victim organisations to facilitate card skimming crimes. Post-crime subversion was evident in nine cases, including Cases 04 and 06. Unlike pre-crime subversion, this describes situations in which subverted individuals were already employed by their respective employers at the time they were subverted by the syndicate.

The purpose of subversion across both the insider and outsider data fell into three broad categories. Facilitative subversion was evident in four cases with subverted actors providing a range of supporting roles including backstopping and approving claims.[302] Third-party subversion was evident in three cases with subverted actors employed by unrelated organisations providing information to the principal fraudster in support of their crimes.[303] Finally, crime subversion was evident in two cases with subverted actors engaged to implement the crimes on behalf of the criminal syndicates.

[302] Case 04 / Case08 / Case 07 / Case 12
[303] Case 05 / Case 06 / Case 13

9.2.4 Intent

Another important observation arising from the analysis of both datasets was the relationship between the time when motivation formed and the corresponding activities associated with accessing the financial system. By way of explanation, insider cases represent instances where individuals gain access to the financial system legitimately and without criminal intent. Then, following that access, criminal intent forms. Conversely, outsider cases represent instances where criminal intent forms before accessing of the target financial system. The significance of this subtle difference in the order in which intent and access occur is that activity traces associated with criminal intent are likely to be left prior to access in the outsider cases, and after access in the insider cases. For example, the outsider who accesses a target financial system after they have formed criminal intent will likely undertake actions to achieve this aim; whereas the insider, already operating within the victim organisation through their position of employment, will not. Therefore, according to Locard's exchange principle, the outsider is likely to leave trace evidence early in their crime.[304] Such trace evidence as it relates to gaining access may include planning-related activities, including the subversion of insiders as already noted; and the preparation of any relevant fraudulent instruments such as fraudulent mortgage applications. In contrast, in the case of the insiders, there is unlikely to be excessive evidence of deliberate activities being undertaken to gain access, principally because access was achieved initially via legitimate means. This suggests that insider crimes are more likely to be opportunistic than are outsider crimes, in support of previous findings (Australian Government, 2016).

9.3 Tradecraft: Learning and Financial Crimes

This section synthesises the insider and outsider data to present key findings from this thesis as they relate to how fraudsters develop the knowledge, skills and expertise that allows

[304] See (Mistek, Fikiet, Khandasammy, & Lednev, 2019)

them to commit their frauds. This section contends that learning across the fraud event timeline varies significantly in terms of what drives the need for learning; what is most likely to be learned at what point in time; and the intensity of the learning at different points in time along the fraud event timeline.

9.3.1 Phases of Criminal Learning

The data analysis in this thesis, as summarised in Table 17, identified nine learning sources spread over three distinct learning phases, defined as:

1. Pre-intent phase: learning that is generic, and evolves through routine daily activities, education and on-the-job learning experiences, all of which occur before the formation of criminal intent.
2. Pre-crime phase: learning that is targeted and deliberate, and occurs to overcome information, knowledge and skills deficiencies. Learning involves focussed research, the subversion of insiders and learning from criminal facilitators before the crime and occurs following the formation of criminal intent.
3. Post-crime phase: learning that is reactive, and triggered by imminent threats to the fraudster or their crime. Learning focusses on ascertaining the nature of perceived or actual threats, and drives OPSEC decision making.

Table 17

Data Synthesis: Learning

	Insider cases	Outsider cases
Pre-intent learning		
Qualifications	X	X
Current and previous roles	X	X
Criminal past		X
Pre-crime and crime learning		
Current and previous roles	X	X
Collaboration	X	X
Trial and error	X	X
Subverting others		X
Research		X
Law enforcement products		X
Criminal facilitators		X
Post-crime learning		
Collaboration	X	

X – indicates a positive correlation between the χ-axis and the γ-axis

9.3.2 Pre-intent Learning

Pre-intent learning in the insider and outsider cases was generally consistent in terms of the learning sources that were exploited. Qualifications, along with current and previous employment, accounted for most of the learning that occurred. However, there was one difference between the insider and outsider cases, as seen in Table 17. Outsiders were able to draw on experiential learning opportunities triggered by previous contact with police.[305] This learning source was evident in six of eight cases,[306] and the implications of this variation were most clearly observed during the post-crime phase. By way of explanation, this thesis theorises that the fraudsters who had previously interacted with police were less likely to

[305] See (Kolb, 2014)
[306] Case 02 / Case 03 / Case 05 / Case 06 / Case 11 / Case 12

require post-crime learning, and thus demonstrated more pre-crime planning activities than those with no previous police contact. The effect of this was that criminally experienced offenders undertook more planning upfront, the result of which means they were less likely to need to cover their tracks after the crime. Logically, outsiders unknown to the financial system would be more easily able to walk away with confidence that their real identity had not been compromised; whereas insiders would be less able to achieve the same anonymity and tend to undertake more learning-related activities during the post-crime phase.

9.3.3 Pre-crime Learning

The pre-crime phase revealed a greater divergence between the insider and outsider cases in terms of the learning sources they exploited. As shown in Table 17, insider cases tended to exploit fewer learning sources than outsider cases. For example, insiders relied on current and previous roles, along with collaboration to satisfy their information needs. There was also one instance where the principal fraudster PF13 and associate fraudster AF13 undertook a deliberate period of trial and error to understand how best to structure their crime to minimise their chances of detection.[307] Outsiders were more likely to exploit a wider range of learning sources than insiders. For example, in addition to learning from current and previous employment, collaboration and trial and error, outsiders drew on criminal facilitators in two cases,[308] subverted others in four cases,[309] undertook research in two cases,[310] drew learning directly from law enforcement products in one case,[311] and relied on previous experiences with law enforcement in six of eight cases.[312]

[307] Case 13
[308] Case 06 / Case 12
[309] Case 01 / Case 03 / Case 06 / Case 12
[310] Case 02 / Case 03
[311] Case 05
[312] Case 02 / Case 03 / Case 05 / Case 06 / Case 11 / Case 12

9.3.4 Crime and Post-crime Learning

The post-crime phase provided the greatest contrast between the insider and outsider cases. Insiders exhibited periods of collaborative learning during the post-crime phase, while outsider learning in this phase was noticeable by its absence. The reason for uptake in collaborative learning across the insider case data was police intervention, as seen in three of five cases,[313] while the commencement of internal investigations was identified in a further two of five cases.[314] Either external law enforcement or internal organisation awareness of the activities of a syndicate triggered an extensive period of reactive learning and this was evident in unplanned and hurried conversations including the swapping of stories linked to co-accuseds' interactions with police officials. This heightened period of activity immediately following their detection was driven by the desire to distance themselves from both the crime and, in some instances, the label of being a criminal.

Analysis of the outsider data, however, revealed something altogether different. Rather than frantic efforts, post-crime learning was noticeable in its absence. The reason for this is potentially complicated, but in the absence of a clear explanation from the data, it is theorised that since outsiders did not hold occupational positions, they felt it was likely to be much harder for police to locate them. Although there is no evidence of this from the outsider cases, intervention would likely trigger a similar period of interaction and reactive learning to that seen in the insider case data.

9.4 Tradecraft: Planning of Financial Crimes

This section synthesises the insider and outsider data to present key findings from this thesis as they relate to how fraudsters plan and prepare for their crimes. The data analysed in this thesis, as summarised in Table 18, identify three temporal phases of planning. Unlike

[313] Case 09 / Case 10 / Case 13
[314] Case 04 / Case 08

pre-intent learning, along with pre-crime learning and post-crime learning as identified in the previous section, no pre-intent planning was evident in the data, given that by its nature, the planning of crime is unlikely to occur before the formation of criminal intent. Despite this, the data show extensive evidence of pre-crime, crime phase and post-crime planning. The data also provide evidence of two common triggers that brought on periods of planning, and one that was unique to the outsider cases. Finally, analysis of the data revealed a range of behaviours that form eight types of criminogenic tradecraft.

Table 18

Data Synthesis: Planning

	Insider	Outsider
Temporal planning phases		
Pre-crime phase	2 of 5 cases	All cases
Crime phase	4 of 5 cases	7 of 8 cases
Post-crime phase	3 of 5 cases	3 of 8 cases
Planning triggers		
Crime initiation planning	2 of 5 cases	All cases
External factors	X	X
Detection of crime	X	X
Tradecraft		
Delegated planning	X	X
Rehearsals and trial runs	X	X
OPSEC	X	X
Manipulating others	X	
Associate roles critical		X
Backstopping		X
Resources		X
Victim selection		X

X – indicates a positive correlation between the χ-axis and the γ-axis

9.4.1 Temporal Planning Phases

The analysis of both the insider and outsider case data revealed that the insiders generally tended to do less planning early in the fraud event timeline, but demonstrated more planning activities towards the end. However, the reverse was true of the outsiders, all of whom demonstrated prolonged periods of pre-crime planning but had all but abandoned such behaviours later in the fraud event timeline.

Insiders, through their position in the victim organisation, were generally better equipped with higher levels of knowledge and access than their outsider counterparts. Based on this finding, it is theorised that the insiders were less likely to demonstrate pre-crime planning-related behaviours, supporting the thesis that insiders are generally opportunistic offenders.[315] However, this was not the rule in every instance as the principal fraudsters in Cases 04 and 13 demonstrated extensive levels of detailed upfront planning. Outsiders, in contrast, who lacked the access and knowledge of their insider contemporaries, were forced to adapt earlier in the fraud event timeline; thus demonstrating higher levels of planning-related activities at the commencement of the crime.

The extent of planning exhibited by insiders and outsiders during the crime phase was broadly similar in terms of the number of cases. Insider cases in which there was little to no pre-crime planning tended to exhibit increased levels of planning activity during the crime phase than those in which there was extensive planning during the pre-crime phase, as was the case with the outsider crimes. Of the 13 cases, 2 were classified as one-off crimes where, from the outset, the intention was to commit a single large fraud.[316] In these crimes, the planning was generally restricted to responding to threats or overcoming controls, as was seen in Case 01, when AF01a commenced a departmental restructure to dismiss the whistle

[315](Australian Government, 2016)
[316] Case 01 / Case 12

blower and prevent the collapse of the fraud. In the remaining 11 ongoing cases, the intention was to continue the offending beyond its first iteration. In these cases, the nature of the planning tended to involve a mix of responding to threats, overcoming controls and replanning for the next cycle of offending.

Finally, the data show far greater levels of post-crime planning in the insider cases than in the outsider cases. Insiders, particularly those with limited criminal maturity who undertook little to no pre-crime planning, were in most instances forced to undertake significant levels of planning to distance themselves from their crimes and hinder subsequent police investigations.[317] Indeed, of the two insider cases where there was no observable post-crime planning, analysis of the data revealed that this was because of the early arrest of the principal fraudster before they became aware they were subject to a police investigation. Outsiders, conversely, demonstrated relatively limited levels of post-crime planning because they were not encumbered by the connection of their employment status and therefore were free to walk away from their crimes.

What this analysis reveals when seeking an answer to the question 'how does planning and preparation differ between insider and outsider cases?', is that the proximity of the principal fraudster to the target financial system influences when planning is more likely to occur along the fraud event timeline. Insiders tended to exhibit low levels of planning initially, but as they moved along their fraud event timeline, their observable levels of planning steadily increased. In contrast, cases where the principal fraudster was an outsider tended to commence with high levels of observable planning; as they progressed along their fraud event timeline, these activities dropped off. The implication of this for financial crime researchers, and indeed those who control fraud in practitioner settings is that it identifies

[317] (Sutherland, 1947)

heightened periods of activity across different temporal planning zones that correspond to the principal fraudster's classification as either an insider or an outsider.

9.4.2 Planning Triggers

The insider and outsider data provide evidence of sudden and often significant increases in the level of planning and decision-making activities that led to the identification of three meta-level classifications of planning triggers. As described in sections 8.1.1 and 8.2.1, a planning trigger sets in motion planning activity. The first stage of the sudden or reactive planning event was the acquisition of knowledge, which was linked to the nature of the planning trigger. For example, the first planning trigger, crime initiation, saw fraudsters seek out information relating to the target financial system, its controls and how access might be arranged. The next planning trigger, external factors, included several situationally specific factors such as end of period contract negotiations or the departure of a critical associate, which required understanding a different set of parameters in each case. The final planning trigger, 'detection of crime, resulted in a concerted effort across all cases where the fraudsters set out to establish how severely they, and their crimes, had been compromised.

Having established baseline knowledge, fraudsters were observed developing objectives, and organising and delegating tasks to meet those objectives. In the case of crime initiation, there were examples of identifying further knowledge and access deficiencies to then recruit associates or subvert insiders.[318] In the external factors cases, there were examples of script rehearsals,[319] identifying new associates,[320] new victims[321] and devising ways to overcome fraud controls.[322] Finally, in the detection of crime cases, there was

[318] Case 02 / Case 03 / Case 04 / Case 05 / Case 06 / Case 11
[319] Case 02 / Case 03 / Case 05 / Case 06 / Case 08 / Case 09
[320] Case 02 / Case 04 / Case 05
[321] Case 02 / Case 03 / Case 06 / Case 07 / Case 10
[322] Case 01 / Case 02 / Case 06

evidence of sharing methods for destroying evidence,[323] devising stories and creating alibis,[324] arranging covert meetings[325] and attempting to remove the threat to the crime.[326]

In both insider and outsider cases, crime initiation was an evident planning trigger; however, it was more prevalent in the outsider dataset where the principal fraudsters lacked the insiders' access to and knowledge of the target financial system. In the second planning trigger classification, external factors were more evenly distributed across both insider and outsider cases and in all cases the resulting behaviour was unique to each case. Finally, detection of crime was a major factor that drove sudden increases in the planning undertaken by fraudsters. This planning trigger was more evident in the insider data with four of five cases revealing some degree of post-detection planning undertaken by insiders;[327] in the outsider cases this was only evident in two of the eight.[328]

9.4.3 Criminal Tradecraft

Analysis of the insider and outsider datasets revealed a range of planning and decision-making outputs. Insiders, secure in their workplace with access to the target financial system and knowledge of how it and the associated fraud controls worked, were less likely to demonstrate behaviours associated with criminal planning. Outsiders displayed a far greater array of planning and decision-making outputs. Insider cases included instances where the planning of the crime, or parts of the crime, was delegated to associate fraudsters,[329] where they undertook trial runs and rehearsals before the commencement of the

[323] Case 03 / Case 04
[324] Case 01 / Case 03 / Case 04 / Case 09 / Case 12
[325] Case 03 / Case 04
[326] Case 01
[327] Case 08 / Case 09 / Case 10 / Case 13
[328] Case 01 / Case 12
[329] Case 08 / Case 13

crime,[330] manipulated others to affect aspects of their crimes[331] and undertook a range of OPSEC activities to either avoid detection or frustrate police investigations.[332]

In addition to the planning and decision-making outputs displayed by the insiders, outsiders also relied heavily on associate fraudsters to undertake critical roles in all cases. As already described, insiders benefited from their occupational position in many ways, while outsiders needed to improvise more often to overcome internal controls and implement their crimes. In many of these instances, outsiders also needed to develop resources with which to implement their crimes.[333] Finally, fraudsters implemented a range of strategies, defined here as backstopping, to legitimise their fraudulent acts in a way that convinced the victim as to the legitimacy of the syndicate's fraudulent representation.

9.5 Summary

The insiders and outsiders in the cases examined in this study shared numerous similarities in how they approached their crimes; however, the differences found to exist between these two cohorts of fraudsters are greater than previously recognised. As the principal variable at the centre of this thesis, proximity to the target financial system had an impact on the way distinct tradecraft practices were deployed across insider and outsider cases.

This chapter has shown that while insiders enjoyed obvious benefits via their occupational positions in victim organisations, they nonetheless demonstrated often complex efforts to gain access to information and organisations systems outside their delegated authority. Additionally, insiders were observed gaining unlawful access to non-victim secondary systems as a critical part of their criminal endeavour. Outsiders worked harder to

[330] Case 13
[331] Case 04 / Case 08 / Case 09 / Case 10
[332] Case 04 / Case 08 / Case 09
[333] Case 02 / Case 03 / Case 05 / Case 06 / Case07 / Case 11 / Case 12

overcome access deficiencies early on in their fraud event timeline. Next, the chapter showed that despite the advantage provided by their occupational position, insiders were regularly forced to acquire more information than they normally used in their legitimate role to facilitate their crimes. Outsiders, again at a disadvantage relative to insiders, drew on a much broader set of learning opportunities as they acquired the necessary information to effect their crimes. Finally, it was evident that the planning processes of insiders differed from those of outsiders: insiders tended to be late crime planners,[334] whereas outsiders tended to be early crime planners.[335]

[334] Late crime planners tended to demonstrate more planning activities towards the end of the fraud event timeline. This, it is asserted, was because insiders by virtue of their positions did less planning at the start of their fraud event timeline.

[335] In contrast to late crime planners, early crime planners demonstrated higher levels of planning-related activities at the very early stages of their fraud event timeline to overcome knowledge and access deficiencies.

Chapter 10: Conclusion

This study aimed to ascertain the extent to which differences in the selection and implementation of a fraudster's tradecraft are influenced by their position as either an insider or an outsider to the target financial system. The study employed a qualitative mixed-methods methodological framework that drew on semi-structured interviews with 13 police detectives from two state and federal law enforcement agencies and the case management files they had compiled as part of their investigations. From this, it can be concluded that the proximity of the principal fraudster to the financial system reliably influences the order in which their tradecraft practices are used in the fulfilment of their criminal enterprise. The results indicate that the advantages enjoyed by insiders who are already proximate to the target financial system and have a greater level of knowledge, also act as a proverbial double-edged sword during the post-crime phase where insiders employ higher rates of task-related backstopping activity than do outsiders. This increased activity, focussed on distancing the insider from their crime, is diametrically opposed to the behaviour patterns of outsiders, who have higher rates of activity early in their crimes to overcome their access and knowledge deficiencies.

The approach adopted in this study was driven by the belief that fraud occurs when a criminal gains access to a target financial system, learns how the target financial system operates, plans their crime and implements it in a manner that lessens their chance of detection. This thesis proposed that the ALPi Model would be useful for identifying and classifying relevant tradecraft practices. This, it was tentatively proposed, might aid in the eventual development and implementation of more effective fraud prevention strategies (Pontell, 2009). The infeasibility of interviewing convicted fraudsters leaves some doubt as to whether the findings of the research are representative of the crimes, as seen through the eyes of the fraudsters. However, the availability of audio surveillance intercept recordings of fraudsters' uninhibited discussions during their planning stages provided confidence in the

validity of the findings. The ALPi Model, as a framework that guided the analysis of insider and outsider cases, meant this study was not dependent on a single crime type, as is the case with similar methodologies.[336] This provided for a larger selection of crimes to be included in the study and thus a greater degree of validity as it related to the findings.

It was expected that the research would confirm the validity of the stated hypothesis that a fraudster's status as either an insider or an outsider to a target financial system would shape the implementation of their tradecraft. It was anticipated that the ALPi Model would make it possible to differentiate between the approaches adopted by insider and outsider fraudsters. However, the diversity of tradecraft practices displayed was unexpected. Similarly, discovery of the potential need for revisions to routine activity theory,[337] the fraud triangle,[338] and the time allocation model of criminal planning was not anticipated.[339] Therefore, the results of this study exceeded the expectations identified at its commencement, and it is suggested that this thesis provides an original contribution to the study of fraud and financial crime.

10.1 Limitations

The limitations of this study include the use of a purposive sampling approach and thematic analysis; data access challenges; inconsistency between cases in the nature, volume and availability of data; data volume in general; and the comparatively small number of cases that made up the final dataset.

The data collection was limited by several factors. The nature of the problem precluded a probability sampling method as the formulated question suggested the need to survey experts with experience in investigating complex financial crimes. This restricted the

[336] See (Cornish, 1993)
[337] See (Cohen & Felson, 1979)
[338] See (Wells, 1997)
[339] See (Allen, 2011)

total number of potential detectives to those with current experience in specialised financial crime units in law enforcement agencies. While efforts were made to avoid the collection of irrelevant data, two cases that didn't meet the selection criteria outlined in section 4.3.2. Consequently, these cases were excluded from the analysis.[340] There was also the possibility that relying solely on detectives' accounts might result in a biased interpretation of fraudsters' actions. Finally, while the results of this thesis provided insight into the activities of the identified sample of fraudsters, it is potentially difficult to infer or generalise the identified tradecraft classifications beyond the sample in the absence of a much larger sample (Barratt, Ferris, & Lenton, 2015).[341]

The nature of the research problem suggested that a thematic analysis of the detective interviews and case management files would provide a comprehensive and robust answer to the research question. However, the flexibility of thematic analysis is a potential limitation when seeking to develop coherent themes based on the interpretation of grammatical units or phrases that can be interpreted differently in diverse contexts (Nowell et al., 2017).

A further data-related limitation is the inconsistent nature and format of the case management files disclosed by the law enforcement agencies. In some instances, full investigative cases were disclosed, including hundreds of hours of intercept data that required transcribing, and a large number of police documents. In other instances, little additional information was provided in support of the detective interviews. This, in most instances, was because of the sensitive nature of the investigations and the risk of exposing police methodology. This resulted in 10 cases being excluded from the final data sample.[342] Finally, despite the number of files that were provided (see Table 4), the reduced number of eligible cases meant that the final dataset was smaller than initially anticipated. Despite this, the study

[340] Case 15 / Case 23
[341] For a fuller discussion see Williamson (2003)
[342] Case 14 / Case 15 / Case 16 / Case 17 / Case 18 / Case 19 / Case 20 / Case 21 / Case 22 / Case 23

findings were reflective of the analysed dataset, and there are opportunities for further research with larger datasets to expand on these findings.

10.2 Future Research

Research should always seek to find an answer to a question. Research should also allow the reader to see possibilities for asking and answering further questions (Baxter, 2014). As this thesis draws to conclusion, it is worth reflecting on the practical, research and theoretical implications that the findings offer in the field of financial crime control.

This thesis has provided several important findings concerning the way proximally divergent fraudsters approach their tradecraft and crime. However, practitioners (detectives etc.) should consider the significance of the diametrically opposed findings regarding insiders' and outsiders' task activity levels, which started low then built across the fraud event timeline for insiders; but started high and progressively lessened for outsiders. Practitioners should consider how differences in these activity outputs might identify not only the proximal nature of the fraudster but also where evidence is more likely to be located. Finally, practitioners should consider the diversity of tradecraft displayed by fraudsters, and the way different tradecraft is used to overcome common financial crime control methodologies. Consequently, these findings present opportunities to refine how financial crimes are prevented, detected and investigated at an operational level.

To better understand the implications of these results, future research might test the capacity of the ALPi Model to elucidate results from a larger dataset. Future research might use the ALPi Model to analyse the access, learning and planning activities of offenders in other crimes; for instance, terrorist or cybercrime cases. Future research might also examine the temporal sequence of tradecraft at distinct stages along the fraud event timeline to ascertain the influence of different tradecraft on the outcome of a criminal endeavour. Research might build on the detail provided in this thesis to examine why crimes are detected

with a focus on identifying consistent causal factors that help unravel such crimes. Specific research might focus on the importance of criminal learning in financial crime settings, an area that requires greater criminological attention.

Future research might also consider how the planning and learning processes evident in the ALPi Model intersect in reactive settings; for instance, if there is an unexpected barrier or prolonged period between detection and arrest. These questions and others that concentrate on the uniqueness of different approaches to committing fraud will aid in revising generalisations that commonly underpin efforts to prevent such crimes. In doing so, such research, building on this thesis will continue to improve the way organisations, legislators and governments approach the topic of financial crime control.

Finally, research provides an opportunity to question established truths that inform our discipline and practice. This thesis provides three insights that may aid in refining the underlying principles that guide the understanding of financial crime. It is suggested that researchers consider the implications of reframing routine activity theory's 'absence of capable guardianship' to a position that recognises a criminal's 'capability to overcome guardianship'; thus acknowledging agency in circumventing fraud controls and bringing tradecraft into the frame.[343] Next, it is suggested that researchers consider the implications of reframing the fraud triangle[344] by way of introducing the ALPi Model as a method of unpacking capability[345] in the new fraud triangle.[346] Given that the original fraud triangle continues to evolve with the intention of more effectively explaining how frauds occur,[347] the ALPi Model is a logical addition to the toolkit available to researchers seeking a more complete picture of the mechanics of financial crime. Finally, it is submitted that future

[343] See (Cohen & Felson, 1979)
[344] See (Wells, 1997)
[345] See (Wolfe & Hermanson, 2004)
[346] See (Kassem & Higson, 2012)
[347] See (Wells, 1997)

research should consider the findings from this thesis as they relate to the propensity of insiders to undertake increased levels of activity during the post-crime phase of their fraud event timeline. Therefore, refining the time allocation model of criminal planning[348] may provide a more balanced view of how fraudsters commit their crimes.

10.3 An Original Contribution to Knowledge

This thesis proposed that greater complexity would be evident in financial crimes than is acknowledged by the literature. It contended that until such complexity is more fully understood, meaningful fraud prevention efforts will remain bereft of their most important asset; that is, a detailed understanding of how fraudsters set about overcoming the controls that organisations and agencies seek to implement. A review of four major criminological theories linked to the study of financial crime, and the associated criminological literature describing a range of crimes, revealed that the specific mechanics of fraud and the tradecraft used has been only rarely examined in detail (Allen, 2011; Benson & Chio, 2019; Braithwaite, 1985; Levi, 1984; Morales et al., 2014; Suh et al., 2020).

Despite the desire to aid in the development of more effective fraud prevention controls, this thesis was deliberately restricted to unpacking the tradecraft deployed by fraudsters during their crimes. The result of this was the identification and description of four temporal activity phases along the fraud event timeline and the presence of three distinct tradecraft classifications. In this way, the introduction of the ALPi Model provided value by describing the observed tradecraft classifications. It offers an innovative method for further examination of fraudsters' tradecraft, thus contributing a fuller understanding of how financial crimes are committed. This micro-level examination of fraud (the ALPi process) unpacks the diversity of fraud tradecraft and addresses the challenge laid down by both Levi (1984) and Braithwaite (1985) to understand the *how* of fraud.

[348] See (Allen, 2011)

In conclusion, this thesis set out to build on several prominent studies that have provided an emerging insight into how fraudsters approach their crimes, via an examination of a series of distinct micro activities (Gill, 2000; Goldstraw-White, 2011; Kenney, 2010a; Pao et al., 2014).[349] This thesis has satisfied that intention via its examination of how fraudsters gain access to targeted financial systems, how system weaknesses are identified, how fraudsters plan to overcome guardianship present, and to what extent they actively engage in OPSEC activities. It is contended that, through this examination of how fraudsters overcome financial systems guardianship, this thesis provides a deeper level of understanding of how fraudsters plan and prepare their crimes, which may aid in advancements in both theory and operational fraud prevention.

[349] Other notable studies are examined in Chapter 3.

References

Acharya, V. V., & Johnson, T. C. (2007). Insider trading in credit derivatives. *Journal of Financial Economics, 84*(1), 110-141. doi:10.1016/j.jfineco.2006.05.003

Agnew, R. (1992). Foundation for a General Strain Theory of crime and delinquency. *Criminology, 30*, 47-87. doi:10.1111/j.1745-9125.1992.tb01093.x

Aguirre, B. E., & Lane, D. (2019). Fraud in disaster: Rethinking the phases. *International Journal of Disaster Risk Reduction, 39*, 101232. doi:10.1016/j.ijdrr.2019.101232

Akers, R. L., & Jensen, G. F. (2007). *Social Learning Theory and the explanation of crime*. New Brunswick: Transaction Publishers.

Akers, R. L., & Sellers, C. S. (2011). *Social Learning Theory*: Oxford University Press.

Alazab, M., & Broadhurst, R. G. (2016). Spam and criminal activity. *Trends & Issues in Crime & Criminal Justice*(526).

Albrecht, C. O., Turnbull, C., Zhang, Y., & Skousen, C. J. (2010). The relationship between South Korean chaebols and fraud. *Managerial Auditing Journal, 33*(3), 1-25. doi:10.1108/01409171011030408

Albrecht, W. S., & Albrecht, C. O. (2004). *Fraud examination and prevention*. Mason: South-Western Educational.

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2006). *Fraud examination*. Mason: South Western Cengage Learning.

Albrecht, W. S., Hill, N. C., & Albrecht, C. C. (2006). The Ethics Development Model applied to declining ethics in accounting. *Australian Accounting Review, 16*(38), 30-40. doi:10.1111/j.1835-2561.2006.tb00323.x

Albrecht, W. S., Howe, K., & Romney, M. B. (1984). *Deterring fraud: The internal auditor's perspective*. Altamonte Springs: Institute of Internal Auditors Research Foundations.

Allan, D. M. C. (2016). The long road to securing our driver's licences. Retrieved from https://www.aspistrategist.org.au/the-long-road-to-securing-our-drivers-licences/

Allan, D. M. C. (2018). Insiders versus outsiders -alternative paths to criminogenic knowledge. In R. G. Smith (Ed.), *AIC research report* (Vol. 10, pp. 35-49). Canberra: Australian Institute of Criminology.

Allan, D. M. C., Kelly, A., & Stephenson, A. (2016). The impact of a changing media landscape on police practice and legitimacy. *Global Media Journal-Australian Edition, 10*(2).

Allan, D. M. C., Kelly, A., & Stephenson, A. (2018). The prominence of fraud in New South Wales metropolitan media reporting. *Crime, Law and Social Change*. doi:10.1007/s10611-018-9784-9

Allen, W. D. (2011). The planning of crime. In *Criminals and victims*: Stanford University Press.

Allingham, M. G., & Sandmo, A. (1972). Income tax evasion: A theoretical analysis. *Journal of Public Economics, 1*(3–4), 323-338. doi:http://dx.doi.org/10.1016/0047-2727(72)90010-2

Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Australian Government (2006).

Antonaccio, O., Smith, W. R., & Gostjev, F. A. (2015). Anomic strain and external constraints: A reassessment of Merton's Anomie/Strain Theory using data from Ukraine. *International Journal of Offender Therapy and Comparative Criminology, 59*(10), 1079-1103. doi:10.1177/0306624X14533071

Appiah, E. (2015). Exploring the perceptions of Northern Virginia accountants on internal control weaknesses resulting in accounting fraud. In S. Robertson, N. Avena, & F. Bearden (Eds.): ProQuest Dissertations Publishing.
Archer, D., & Gartner, R. (1984). *Violence and crime in cross-national perspective*. New Haven: Yale University Press.
Association of Certified Fraud Examiners. (2008). *Profiling a white-collar criminal*. Retrieved from http://www.acfe.com/press-release.aspx?id=4294968561
Association of Certified Fraud Examiners. (2014). *The statistical profile of a fraudster*. Retrieved from https://www.fraud-magazine.com/article.aspx?id=4294984634
Australian Broadcasting Corporation. (2011). Fraud bail hearing for McGurk associate delayed. Retrieved from https://www.abc.net.au/news/2011-07-08/fraud-bail-hearing-for-mcgurk-associate-delayed/2786976
Australian Competition and Consumer Commission. (2021). Losses reported to Scamwatch exceed $211 million, phone scams exploding. *2021*(5th October 2021). Retrieved from https://www.scamwatch.gov.au/news-alerts/losses-reported-to-scamwatch-exceed-211-million-phone-scams-exploding
Australian Government. (2016). *Managing the insider threat to your business: A personnel security handbook*. Canberra: Australian Government
Australian National University. (2021). Policy: Responsible conduct of research. Retrieved from https://policies.anu.edu.au/ppl/document/ANUP_007402
Avortri, C., & Agbanyo, R. (2020). Determinants of management fraud in the banking sector of Ghana: The perspective of the Diamond Fraud Theory. *Journal of Financial Crime, ahead-of-print*(ahead-of-print). doi:10.1108/JFC-06-2020-0102
Axinn, W. G., & Pearce, L. D. (2006). *Mixed-method data collection strategies*. New York: Cambridge University Press.
Ayling, J. (2009). Criminal organizations and resilience. *International Journal of Law, Crime and Justice, 37*(4), 182-196. doi:10.1016/j.ijlcj.2009.10.003
Baker, W. E., & Faulkner, R. R. (2003). Diffusion of fraud: Intermediate economic crime and investor dynamics. *Criminology, 41*(4), 34. Retrieved from https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1745-9125.2003.tb01017.x
Barra, R. A., Savage, A., & Im, E. (2020). Mathematical formulation of the effectiveness of 'Separation of Duties' as a preventive control activity. *Journal of forensic accounting research*. doi:10.2308/JFAR-19-012
Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field methods, 27*(1), 3-21. doi:10.1177/1525822X14526838
Baxter, D. N. (2014). Who is taking the shirt off your back? A multi-method analysis of theft at a specialty retailer. In. Indiana: ProQuest Dissertations Publishing.
Beauregard, E., Leclerc, B., & Lussier, P. (2012). Decision making in the crime commission process: Comparing rapists, child molesters, and victim-crossover sex offenders. *Criminal Justice and Behavior, 39*(10), 1275-1295. doi:10.1177/0093854812453120
Becker, G. S. (1962). Irrational behaviour and Economic Theory. *The Journal of Political Economy, 70*(1), 13.
Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*(2), 169-217. doi:10.2307/1830482
Bennett, T., & Wright, R. (1984). *Burglars on burglary*. Aldershot: Gower Publishing Company Limited.
Benson, M. L. (1985). Denying the guilty mind: Accounting for involvement in a white-collar crime. *Criminology, 23*(4), 9.

Benson, M. L. (2020). Theoretical and empirical advances in the study and control of white-collar offenders. *Justice Evaluation Journal*, 1-20. doi:10.1080/24751979.2020.1808855
Benson, M. L., & Chio, H. L. (2019). Who commits occupational crimes? In M. L. Rorie (Ed.), *The handbook of white-collar crime* (pp. 113-126). Hoboken: Wiley-Blackwell.
Benson, M. L., & Simpson, S. S. (2009). *White-collar crime: An opportunity perspective*. New York: Taylor & Francis.
Benson, M. L., & Simpson, S. S. (2018). *White-collar crime: An opportunity perspective*. New York: Routledge.
Bernard, T. J., Snipes, J. B., & Gerould, A. L. (2016). *Vold's theoretical criminology* (7th ed.). New York: Oxford.
Best, R. A. (2011). *Intelligence information: Need-to-know vs. need-to-share*. Retrieved from Washington DC: https://sgp.fas.org/crs/intel/R41848.pdf
Biggerstaff, L., Cicero, D., & Wintoki, M. B. (2020). Insider trading patterns. *Journal of Corporate Finance, 64*, 101654. doi:10.1016/j.jcorpfin.2020.101654
Birkbeck, C., & Lafree, G. (1993). The situational analysis of crime and deviance. *Annual Review of Sociology, 19*, 113.
Boeije, H. R. (2002). A purposeful approach to the constant comparative method in the analysis of qualitative interviews. *Quality & quantity, 36*(4), 391-409. doi:10.1023/A:1020909529486
Boudon, R. (1998). Limitations of Rational Choice Theory. *American Journal of Sociology, 104*(3), 817-828. Retrieved from http://ezproxy.csu.edu.au/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=2147973&site=ehost-live
Bourgeois, C. A., & Fisher, M. L. (2018). More "bros," more "woes?": The prevalence of male coalitions in crimes of robbery. *Evolutionary Behavioural Sciences, 12*(2), 126-131. doi:10.1037/ebs0000116
Bowen, G. A. (2008). Naturalistic inquiry and the saturation concept: A research note. *Qualitative research: QR, 8*(1), 137-152. doi:10.1177/1468794107085301
Bradford, M., Henderson, D., Baxter, R. J., & Navarro, P. (2020). Using generalized audit software to detect material misstatements, control deficiencies and fraud: How financial and IT auditors perceive net audit benefits. *Managerial Auditing Journal, 35*(4), 521-547. doi:10.1108/MAJ-05-2019-2277
Bradley, H. (2021). Burner phones, fake sources and 'evil twin' attacks: Journalism in the surveillance age. In. London (UK): Guardian News & Media Limited.
Braithwaite, J. (1985). White-collar crime. *Annual Review of Sociology, 11*, 1-25.
Brantingham, P. J., & Brantingham, P. L. (1981). Notes on the geometry of crime. In P. L. Brantingham & P. J. Brantingham (Eds.), *Environmental criminology*. London: Sage.
Brantingham, P. J., & Brantingham, P. L. (1984). *Patterns in crime*. New York: MacMillan.
Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. doi:10.1191/1478088706qp063oa
Brennen, B. S. (2017). *Qualitative research methods for media studies* (2nd edition. ed.). Milton: Taylor and Francis.
Brewer, P. (2020, 13th May). Police refocus on protecting businesses shuttered because of the coronavirus. *The Canberra Times*. Retrieved from https://www.canberratimes.com.au/story/6718517/virus-led-property-crime-shift-prompts-act-police-to-refocus/
Brezina, T., & Topalli, V. (2012). Criminal self-efficacy: Exploring the correlates and consequences of a "successful criminal" identity. *Criminal Justice and Behavior, 39*(8), 1042-1062. doi:10.1177/0093854812438345

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International journal of cyber criminology, 8*(1), 1-20.

Brown, J. (2015, 15 June 2015). Statewide crackdown on card skimmers: Police. *The Maitland Mercury*.

Brown, R. (2017). Vehicle crime prevention and the co-evolutionary arms race: Recent offender countermoves using immobiliser bypass technology. *Security Journal, 30*(1), 60-73. doi:10.1057/s41284-016-0001-1

Burgess, R. L., & Akers, R. L. (1966). A Differential Association-Reinforcement Theory of criminal behaviour. *Social Problems, 14*, 128-147.

Butler, J. B., & Raiborn, C. (2015, July). Fraud: an ounce of prevention. *Cost Management, 29(4)*, 38-48. Retrieved from https://search.proquest.com/docview/1701877105?accountid=10344

https://csulibrary.primo.exlibrisgroup.com/discovery/openurl?institution=61CSU_INST&vid=61CSU_INST:61CSU&aufirst=Janet&aulast=Butler&atitle=FRAUD%3A+AN+OUNCE+OF+PREVENTION&title=FRAUD%3A+AN+OUNCE+OF+PREVENTION&volume=29&date=Jul%2FAug+2015&spage=38&issn=

Button, M., & Brooks, G. (2009). "Mind the gap": Progress towards developing anti-fraud culture strategies in UK central government bodies. *Journal of Financial Crime, 16*(3), 229-244. doi:10.1108/13590790910971784

Campbell, C. (2006). Last resort loans: Unregulated and illegal, payday lenders come under fire. *Maclean's (Toronto), 119*(14), 26.

Canter, D., & Alison, L. (Eds.). (2000). *The social psychology of crime: Groups, teams and networks*. Aldershot: Ashgate.

Carnegie Mellon University. (2012). *Insider fraud in financial services: Illicit cyber activity involving fraud in the U.S. financial services sector*. Retrieved from Pittsburgh: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=27971

Carroll, J., & Weaver, F. (1986). Shoplifters' perceptions of crime opportunities: A process-tracing study. In D. B. Cornish & R. V. Clark (Eds.), *The reasoning criminal: Rational choice perspectives on offending*. New York: Springer-Verlag.

Centre for the Protection of National Infrustructure. (2013). *CPNI insider data collection study: Report of main findings*. Retrieved from London: https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf

Chabinsky, S. R. (2010). The cyber threat: Who's doing what to whom? [Press release]. Retrieved from https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom

Chaikin, D. (2009). Risk-based approaches to combatting financial crime. *Journal of Law and Financial Management, 15*(3), 12.

Chaikin, D. (2018). Blowing the whistle - no rewards please! *Journal of Financial Crime, 25*(3), 2.

Chang, Y.-C. (2010). *Cybercrime across the Taiwan Strait: Regulatory responses and crime prevention.* (Doctor of Philosophy). Australian National University, Canberra.

Choi, K., Lee, J.-l., & Chun, Y.-t. (2017). Voice phishing fraud and its modus operandi. *Security Journal, 30*(2), 454-466. doi:10.1057/sj.2014.49

Clarke, R. V., & Cornish, D. B. (1983). *Crime control in Britain: A review of policy and research*. Albany, NY: State University of New York Press.

Cloward, R. A., & Ohlin, L. E. (1970). Differentiated structures, differential opportunities, and delinquent subcultures. In C. A. Bersani (Ed.), *Crime and delinquency: A reader* (pp. 152-170). London: The Macmillian Company Cillier-Macmillian Limited.
Coenen, T. (2008). *Essentials of corporate fraud*. New Jersey: John Wiley & Sons.
Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. Retrieved from http://ezproxy.csu.edu.au/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=heh&AN=14765415&site=ehost-live
Cohen, S. (2001). *States of denial: Knowing about atrocities and suffering*. Cambridge: Polity.
Cornish, D. B. (1993). *Crime as scripts*. Paper presented at the Second annual seminar on environmental criminology and crime analysis, University of Miami.
Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies, 3*, 46.
Cornish, D. B., & Clarke, R. V. (1986). *The reasoning criminal*. New York: Springer-Verlag.
Cornish, D. B., & Clarke, R. V. (2006). The rational choice perspective. In S. Henry & M. M. Lanier (Eds.), *The essential criminology reader*. Bolder, CO: Westview Press.
Crawford, A., & Evans, K. (2012). Crime prevention and community safety. In M. Maguire, R. Morgan, & R. Reiner (Eds.), *The Oxford handbook of criminology* (pp. 769-805).
Cressey, D. R. (1950). The criminal violation of financial trust. *American Sociological Review, 15*(6), 6. Retrieved from http://ezproxy.csu.edu.au/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=heh&AN=12800650&site=ehost-live
Cressey, D. R. (1953). *Other people's money*. Montclair, NJ: Patterson Smith.
Cressey, D. R. (1960). Epidemiology and individual conduct: A case from criminology. *Pacific Sociological Review, 3*(2), 47-58. Retrieved from <Go to ISI>://WOS:A1960CKY7600001
Cressey, D. R. (1973). *Introduction to the reprint edition. Other people's money: A study in the social psychology of embezzlement* (2 ed.). Montclair, N.J: Pattersin Smith.
Creswell, J. W., & Clark, V. L. P. (2007). *Designing and conducting mixed methods research*. Thousand Oaks: Sage Publications.
Cromwell, P. F., Olson, J. N., & Avary, D. A. W. (1991). *Breaking and entering: An ethnographical analysis of burglary* (Vol. 8). London: Sage Publications.
D'Alessio, S., & Stolzenbery, L. (1990). A crime of convenience: The environment and convenience store robbery. *Environment and Behaviour, 22*(2), 255-271.
de Jonge, J. (2012). *Rethinking Rational Choice Theory: A companion on rational and moral action*. Basingstoke: Palgrave Macmillan.
DeLiema, M. (2018). Elder fraud and financial exploitation: Application of Routine Activity Theory. *The Gerontologist, 58*(4), 706-718. doi:10.1093/geront/gnw258
DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2020). Financial fraud among older Americans: Evidence and implications. *The Journals of Gerontology, 75*(4), 861-868. doi:10.1093/geronb/gby151
Dellaportas, S. (2013). Conversations with inmate accountants: Motivation, opportunity and the Fraud Triangle. *Accounting Forum, 37*(1), 29-39.
Ditton, J. (2001). Commercial robbery: Offenders' perspectives on security and crime prevention. By Martin Gill (London: Blackstone Press, 2000. x + 206pp.). *The British Journal of Criminology, 41*(1), 204-206.
Doig, A., & Sproat, P. A. (2020). Local responses to a national initiative on organised crime and local government procurement fraud. *Journal of Financial Crime, 27*(1), 78-91. doi:10.1108/JFC-12-2018-0129

Dorminey, J. W., Fleming, A. S., Kranacher, M.-J., & Riley, R. A. (2010). Beyond the Fraud Triangle. *The CPA Journal*, *80*(7), 8.
Dorminey, J. W., Fleming, A. S., Kranacher, M.-J., & Riley, R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education*, *27*(2), 555-579. doi:10.2308/iace-50131
Durkheim, E. (1952). *Suicide: A study in sociology* (J. A. Spaulding & G. Simpson, Trans. G. Simpson Ed.). London: Routledge & Kegan.
Durkheim, E. (1982). *The rules of sociological method* (W. D. Halls, Trans. S. Lukes Ed.). London: Macmillan.
Edelhertz, H. (1970). *The nature, impact, and prosecution of white-collar crime*. Washington DC: National Institute of Law Enforcement and Criminal Justice,.
Einhorn, H. J., & Hogarth, R. M. (1981). Behavioural Decision Theory: Processes of judgement and choice. *Annual Review of Psychology*, *32*(1), 53-88. Retrieved from http://ezproxy.csu.edu.au/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=pbh&AN=12446690&site=ehost-live
Ekblom, P., & Tilley, N. (2000). Going equipped: Criminology, situational crime prevention and the resourceful offender. *The British Journal of Criminology*, *40*(3), 376-398.
Empey, L. T., & Stafford, M. C. (1991). *American delinquency, its meaning and construction* (3rd ed.). Belmont: Wadsworth.
Fathi, W. N. I. W. M., Ghani, E. K., Said, J., & Puspitasari, E. (2017). Potential employee fraud scape in Islamic banks: The Fraud Triangle perspective. *Global Journal Al-Thaqafah*, *7*(2), 79-93.
Federal Bureau of Investigation. (1976). *Crime in the U.S.: Uniform crime report*. Retrieved from Washington: https://www.fbi.gov/services/cjis/ucr
Felson, M., & Boba, R. (2010). *Crime and everyday life* (4th ed.). Thousand Oaks: Sage.
Felson, M., Jiang, S., & Xu, Y. (2020). Routine activity effects of the Covid-19 pandemic on burglary in Detroit, March, 2020. *Crime Science*, *9*(1), 10-10. doi:10.1186/s40163-020-00120-x
Fisse, B., & Braithwaite, J. (1983). *The impact of publicity on corporate offenders*. Albany, NY: State University of New York.
Foucault, T., Hombert, J., & RoŞU, I. (2016). News trading and speed. *The Journal of finance (New York)*, *71*(1), 335-382. doi:10.1111/jofi.12302
Franklin, B. (1736). Protection of towns from fire. *The Pennsylvania Gazette*.
Free, C. (2015). Looking through the Fraud Triangle: A review and call for new directions. *Meditari Accountancy Research*, *23*(2), 175-196.
Gambetta, D. (2009). *Codes of the underworld: How criminals communicate*. Princeton: Princeton University Press.
Geis, G. L. (1970). White-collar crime: The heavy electrical equipment antitrust cases of 1961. In C. A. Bersani (Ed.), *Crime and delinquency: A reader* (pp. 170-185). London: The McMillian Company Collier-Macmillian Limited.
Geis, G. L., & Edelhertz, H. (1972). Criminal law and consumer fraud: A sociolegal view. *American Law Review*, *11*, 25.
Ghazi-Tehrani, A. K., & Pontell, H. N. (2015). Corporate crime and state legitimacy: The 2008 Chinese melamine milk scandal. *Crime, law, and social change*, *63*(5), 247-267. doi:10.1007/s10611-015-9567-5
Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing evolves: Analyzing the enduring cybercrime. *Victims & offenders*, *16*(3), 316-342. doi:10.1080/15564886.2020.1829224
Gibbs, J. P. (1987). The state of criminological theory. *Criminology*, *25*(4), 821-840. doi:10.1111/j.1745-9125.1987.tb00821.x

Gill, M. (2000). *Commercial robbery: Offenders' perspectives on security and crime prevention* London: Blackstone.
Gill, S. L. (2020). Qualitative sampling methods. *Journal of human lactation, 36*(4), 579-581. doi:10.1177/0890334420949218
Gillham, B. (2005). *Research interviewing the range of techniques*. Maidenhead: Open University Press.
Gilmour, N. (2014). Understanding money laundering - A crime script approach. *The European Review of Organised Crime, 1*(2), 21.
Ginsberg, H., & Opper, S. (1988). *Piaget's Theory of Intellectual Development*. New Jersey: Prectice-Hall Inc.
Glueck, S. (1956). Theory and fact in criminology. *The British Journal of Delinquency, 7*(2), 92-109.
Goldstraw-White, J. (2011). *White-collar crime: Accounts of offending behaviour*. Basingstoke: Palgrave Macmillan.
Gomzin, S. (2014). *Hacking point of sale: Payment application secrets, threats, and solutions* (1st edition ed.). Indianapolis, IN: John Wiley and Sons.
Goode, S., & Lacey, D. (2011). Detecting complex account fraud in the enterprise: The role of technical and non-technical controls. *Decision Support Systems, 50*(4), 702-714. doi:10.1016/j.dss.2010.08.018
Gottschalk, P. (2018). Negative organizational dynamics as an enabler of white-collar crime. *International Journal of Police Science & Management, 20*(2), 116-123. doi:10.1177/1461355718763455
Grabosky, P. N., Braithwaite, J., & Wilson, P. R. (1987). The myth of community tolerance toward white-collar crime. *Australian and New Zealand Journal of Criminology, 20*, 33-44.
Grabosky, P. N., & Sutton, A. (1989). *Stains on a white-collar: Fourteen studies in corporate crime or corporate harm*. Australia: Federation Press.
Grabosky, P. N., & Walkley, S. (2007). Computer crime and white-collar crime. In H. N. Pontell & G. Geis (Eds.), *International handbook of white-collar and corporate crime*. New York: Springer Science and Business Media.
Gray, G. C. (2013). Insider accounts of institutional corruption: Examining the social organization of unethical behaviour. *The British Journal of Criminology, 53*(4), 533-551. doi:10.1093/bjc/azt013
Haelterman, H. (2016). *Crime script analysis: Preventing crimes against business*. London: Palgrave Macnillian.
Harbinson, E. (2020). Investigating women and men convicted of white-collar offences on federal community supervision: Sample and methods. *Criminal justice studies, 33*(1), 4-12. doi:10.1080/1478601X.2020.1709949
Hardy, J., Bell, P., & Allan, D. M. C. (2020). A crime script analysis of the Madoff investment scheme. *Crime Prevention and Community Safety*, 30. doi:10.1057/s41300-019-00082-6
Hataley, T. (2020). Trade-based money laundering: Organized crime, learning and international trade. *Journal of Money Laundering Control, 23*(3), 651-661. doi:10.1108/JMLC-01-2020-0004
Hawley, A. (1950). *Human ecology: A theory of community structure*. New York: Ronald.
Hayne, K. M. (2018). *Interim report: Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry*. Canberra: Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry
Henry, S., & Einstadter, W. J. (2006). *Criminological theory: An analysis of its underlying assumptionsCriminological theory* (2nd ed. ed.).

Herndon, T. (2019). Liar's loans, mortgage fraud, and the Great Recession. *Review of political economy, 31*(4), 479-508. doi:10.1080/09538259.2020.1747746
Hesse-Biber, S. (2010). Qualitative approaches to mixed methods practice. *Qualitative Inquiry, 16*(6), 455-468.
Hipp, J. R., Kim, Y.-A., & Wo, J. C. (2020). Micro-scale, meso-scale, macro-scale, and temporal scale: Comparing the relative importance for robbery risk in New York City. *Justice Quarterly*, 1-25. doi:10.1080/07418825.2020.1730423
Holloway, I., & Todres, L. (2003). The status of method: Flexibility, consistency and coherence. *Qualitative research: QR, 3*(3), 345-357. doi:10.1177/1468794103033004
Holmes, A. G. D. (2020). Researcher positionality - a consideration of its influence and place in qualitative research - a new researcher guide. *International Journal of Education, 8*(4), 10. doi:https://doi.org/10.34293/education.v8i4.3232
Huang, S., Lin, C.-C., Chiu, A.-A., & Yen, D. (2017). Fraud detection using Fraud Triangle risk factors. *Information Systems Frontiers, 19*(6), 1343-1356. doi:10.1007/s10796-016-9647-9
Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *The British Journal of Criminology, 55*(3), 596-614. doi:10.1093/bjc/azu106
Jacobs, B. A. (1996). Crack dealers and restrictive deterrence: Identifying narcs. *Criminology, 34*(3), 409-431. doi:10.1111/j.1745-9125.1996.tb01213.x
Jacobs, B. A. (2010). Serendipity in robbery target selection. *The British Journal of Criminology, 50*(3), 514-529. doi:10.1093/bjc/azq002
Jaques, S., & Reynald, D. M. (2011). The offenders' perspective on prevention: Guarding against victimization and law enforcement. *Journal of Research in Crime and Delinquency, 49*(2), 269-294. doi:10.1177/0022427811408433
Jensen, G. F. (1972). Parents, peers, and delinquent action: A test of the Differential Association perspective. *The American Journal of Sociology, 78*(3), 562-575. doi:10.1086/225364
Joffe, H. (2011). Thematic analysis. In D. Harper & A. R. Thompson (Eds.), *Qualitative research methods in mental health and psychotherapy* (pp. 209-223). Chichester, UK: Wiley-Blackwell.
Johnston, R., & Spencer, R. (2011). The right internal controls prevent fraud and loss. *Financial Executive, 27*(6), 60-63.
Jones, N. P. (2019). Bacterial conjugation as a framework for the homogenization of tactics in Mexican organized crime. *Studies in Conflict & Terrorism*, 1-30. doi:10.1080/1057610X.2019.1586356
Jones, P. C., & Tickner, P. (2004). *Fraud and corruption in public services: A guide to risk and prevention*: Gower.
Kassem, R. (2018). Exploring external auditors' perceptions of the motivations behind management fraud in Egypt: A mixed-methods approach. *Managerial Auditing Journal, 33*(1), 16-34. doi:10.1108/MAJ-11-2016-1470
Kassem, R., & Higson, A. (2012). The new Fraud Triangle model. *Journal of Emerging Trends in Economics and Management Sciences, 3*(3), 191-195.
Katselas, D. (2018). Insider trading in Australia: Contrarianism and future performance. *Pacific-Basin Finance Journal, 48*, 112-128. doi:10.1016/j.pacfin.2018.01.004
Kawasaki, T. (2019). Review of comparative studies on white-collar crime and corporate crime. In M. L. Rorie (Ed.), *The handbook of white-collar crime* (pp. 437-447).
Kembrey, M. (2016, 15th July 2016). Former fraud investigator Wayne Hancock to be sentenced over Manly Eagles free phones. *Sydney Morning Herald*. Retrieved from https://www.smh.com.au/national/nsw/former-fraud-investigator-wayne-hancock-to-be-sentenced-over-manly-eagles-free-phones-20160715-gq6p7c.html

Kemp, L., Zolghadriha, S., & Gill, P. (2019). Pathways into organized crime: Comparing founders and joiners. *Trends in Organized Crime*, 1-24. doi:10.1007/s12117-019-09371-w
Kendall, R. E. (2004). Financial crime, terror and subversion. *Journal of Financial Crime, 11*(4), 363-365. doi:10.1108/13590790410809356
Kenney, M. (2009). *Organizational learning and Islamic militancy*. Retrieved from Washington: https://www.ojp.gov/ncjrs/virtual-library/abstracts/organizational-learning-and-islamic-militancy
Kenney, M. (2010a). Beyond the internet: Mētis, techne, and the limitations of online artifacts for Islamist terrorists. *Terrorism and Political Violence, 22*(2), 177-197. doi:10.1080/09546550903554760
Kenney, M. (2010b). "Dumb" yet deadly: Local knowledge and poor tradecraft among Islamist militants in Britain and Spain. *Studies in Conflict & Terrorism, 33*(10), 911-932. doi:10.1080/1057610X.2010.508508
Kim, S., & Nigel, M. (2008). Commuter finds secret al-Qa'ida report on train. *The Independent (London, England)*, 2.
Kleck, G., Tark, J., & Bellows, J. J. (2006). What methods are most frequently used in research in criminology and criminal justice? *Journal of Criminal Justice, 34*(2), 147-152. doi:10.1016/j.jcrimjus.2006.01.007
Knowles, G. J. (1999). Deception, detection, and evasion: A trade craft analysis of Honolulu, Hawaii's street crack-cocaine traffickers. *Journal of Criminal Justice, 27*(5), 443-455. doi:10.1016/S0047-2352(99)00015-X
Kolb, D. A. (2014). *Experiential learning: Experience as the source of learning and development* (2nd ed.). Englewood Cliffs, N.J.: Prentice-Hall.
Komesar, N. K. (1973). A theoretical and empirical study of victims of crime. *The Journal of Legal Studies, 2*(2), 301-321. doi:10.1086/467500
Kornhauser, R. (1963). *Theoretical issues in the sociological study of juvenile delinquency*. Center for the Study of Law and Society, Berkley.
Kornhauser, R. (1978). *Social sources of delinquency*. Chicago: University of Chicago Press.
Kranacher, M.-J., Riley, R. A., & Wells, J. T. (2011). *Forensic accounting and fraud examination*. Hoboken, N.J: John Wiley.
Kroneberg, C., & Kalter, F. (2012). Rational Choice Theory and empirical research: Methodological and theoretical contributions in Europe. *Annual Review of Sociology, 38*, 25.
Kubrin, C. E., Stucky, T. D., & Krohn, M. D. (2009). *Researching theories of crime and deviance*. Oxford: Oxford University Press.
Lacoste, J., & Trembley, P. (2003). Crime and innovation: A script analysis of patterns in cheque forgery. *Theory for Practice in Situational Crime Prevention, 16*.
Lane, B. R., Salmon, P. M., Desmond, D., Cherney, A., Carley, A., Hulme, A., & Stanton, N. A. (2020). Out of control?: Using STAMP to model the control and feedback mechanisms surrounding identity crime in darknet marketplaces. *Applied ergonomics, 89*, 103223. doi:10.1016/j.apergo.2020.103223
Langton, L., & Piquero, N. L. (2007). Can General Strain Theory explain white-collar crime? A preliminary investigation of the relationship between strain and select white-collar offences. *Journal of Criminal Justice, 35*(1), 1-15. doi:https://doi.org/10.1016/j.jcrimjus.2006.11.011
Lanier, M. M., Henry, S., & Anastasia, D. J. M. (2004). *Essential criminology*(4th ed.).
Lashmar, P., & Hobbs, D. (2018). Diamonds, gold and crime displacement: Hatton Garden and the evolution of organised crime in the UK. *Trends in Organized Crime, 21*(2), 20.

Laufer, D. (2011). Small business entrepreneurs: A focus on fraud risk and prevention. *American Journal of Economics and Business Administration, 3*(2), 401-404. Retrieved from http://search.proquest.com/docview/1025014883?accountid=10344
Lemert, E. M. (1964). Social structure, social control and deviation. In C. M. B (Ed.), *Anomie and deviant behaviour* (pp. 59-60). New York: Free Press.
Levi, M. (1981). *The phantom capitalist: The organisation and control of long-firm fraud*. London: Heinemann.
Levi, M. (1984). Giving creditors the business: dilemmas and contradictions in the organisation of fraud. *International Journal of the Sociology of Law, 12*, 321-333.
Levi, M. (1993). White-collar crime: The British scene. *Annals of the American Academy of Political and Social Science, 525*, 71-82.
Levi, M. (2008). *The phantom capitalist: The organisation and control of long-firm fraud*: Ashgate Pub Co.
Levi, M. (2010a). Financial crimes in comparative context. In S. Shoham, Giora, P. Knepper, & M. Kett (Eds.), *International handbook of criminology* (pp. 309-342). Boca Raton: FL: CRC Press.
Levi, M. (2010b). Serious tax fraud and noncompliance. *Criminology & Public Policy, 9*(3), 21.
Levi, M. (2011). International fraud. In M. Natarajan (Ed.), *International crime and justice*. New York: Cambridge University Press.
Levi, M. (Ed.) (1999). *Fraud: Organization, motivation and control* (Vol. 1). Aldershot: Ashgate.
Levi, M., Nelen, H., & Lankhorst, F. (2005). Lawyers as crime facilitators in Europe: An introduction and overview. *Crime, Law and Social Change, 42*(2), 117-121. doi:10.1007/s10611-005-5654-3
Lewis, L. S. (2013a). The confidence game: Backstage, the accomplices. *Society (New Brunswick), 50*(4), 365-378. doi:10.1007/s12115-013-9675-8
Lewis, L. S. (2013b). The confidence game: Madoff and the 17th floor ensemble. *Society (New Brunswick), 50*(5), 493-502. doi:10.1007/s12115-013-9698-1
Lokanan, M. E. (2015). Challenges to the Fraud Triangle: Questions on its usefulness. *Accounting Forum, 39*(3), 201/224.
Lokanan, M. E. (2018). Informing the Fraud Triangle: Insights from Differential Association Theory. *The Journal of Theoretical Accounting Research, 14*(1), 55-98.
Maimon, D., Howell, C. J., Moloney, M., & Park, Y. S. (2020). An examination of email fraudsters' modus operandi. *Crime & Delinquency*. doi:10.1177/0011128720968504
Maluleke, W., Motseki, M. M., Mokwena, R. J., & Dlamini, S. (2021). The modus operandi of perpetrators for credit card fraud in the Vaal Region, South Africa. *Cogent social sciences, 7*(1), 1930337. doi:10.1080/23311886.2021.1930337
Marcum, C. D. (2009). *Adolescent online victimization A test of Routine Activities Theory*. El Paso: LFB Scholarly Publishing LLC.
Marengo, L., & Dosi, G. (2005). Division of labor, organizational coordination and market mechanisms in collective problem-solving. *Journal of Economic Behaviour & Organization, 58*(2), 303-326. doi:10.1016/j.jebo.2004.03.020
Marques, J., & Dhiman, S. (Eds.). (2018). *Engaged leadership transforming through future-oriented design thinking* (1st ed. 2018. ed.). Cham: Springer International Publishing.
Matsueda, R. L. (1982). Testing Control Theory and Differential Association: A causal modeling approach. *American Sociological Review, 47*(4), 489-504. doi:10.2307/2095194
Matsueda, R. L. (1988). The current state of Differential Association Theory. *Crime & Delinquency, 34*(3), 277-306.

Maulidi, A. (2020). When and why (honest) people commit fraudulent behaviours?: Extending the Fraud Triangle as a predictor of fraudulent behaviours. *Journal of Financial Crime, 27*(2), 541-559. doi:10.1108/JFC-05-2019-0058
Maulidi, A., & Ansell, J. (2021). Tackling practical issues in fraud control: A practice-based study. *Journal of Financial Crime, 28*(2), 493-512. doi:10.1108/JFC-07-2020-0150
Mayo, E. (1933). *The human problems of an industrial civilization*. New York: The Macmillan Company.
Mayo, E. (1986). *The human problems of an industrial civilization*. Salam, Hampshire: Ayer Co., Publishers.
McCarthy, B., Hagan, J., & Cohen, L. E. (1998). Uncertainty, cooperation, and crime: Understanding the decision to co-offend. *Social Forces, 77*, 155-176.
McClymont, K. (2012). International men of mystery. *Sydney Morning Herald*. Retrieved from https://www.smh.com.au/national/international-men-of-mystery-20121203-2apqd.html
McFadden, D. (2001). Economic choices. *American Economic Review, 91*(3), 351-378. doi:10.1257/aer.91.3.351
McFarlane, J. (2001). Corruption and the financial sector: The strategic impact. *Journal of Financial Crime, 9*(1), 8-21. doi:10.1108/eb026002
McGlynn, P., & Garner, G. (2019). *Intelligence analysis fundamentals*. Boca Raton: CRC Press, Taylor & Francis Group.
McGrath, J. (2020). 'Walk softly and carry no stick': Culture, opportunity and irresponsible risk-taking in the Irish banking sector. *European Journal of Criminology, 17*(1), 86-105.
McLaughlin, E., & Muncie, J. (2006). *The Sage dictionary of criminology*. London: Sage.
Meenaghan, A., Nee, C., Van Gelder, J. L., Vernham, Z., & Otte, M. (2020). Expertise, emotion and specialization in the development of persistent burglary. *The British Journal of Criminology, 60*(3), 742-761. doi:10.1093/bjc/azz078
Meier, R. F., & Miethe, T. (1993). Understanding theories of criminal victimization. In M. Tonry (Ed.), *Crime and justice: An annual review of research*. Chicago: University of Chicago.
Meloni, O. (2014). Does poverty relief spending reduce crime? Evidence from Argentina. *International Review of Law & Economics, 39*(C), 28-38. doi:10.1016/j.irle.2014.05.002
Merton, R. K. (1938). Social structure and anomie. *American Sociological Review, 3*(5), 672-682. Retrieved from http://ezproxy.csu.edu.au/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=heh&AN=12781867&site=ehost-live
Merton, R. K. (1968). *Social theory and social structure: 1968 enlarged edition*. New YorK: The Free Press.
Merton, R. K. (1969). Social Structure and Anomie. In D. R. Cressey (Ed.), *Delinquency, crime and social processes* (pp. 254-284). New York: Harper & Row, Publishers.
Messerli, T. C. (2020). Ocean's Eleven scene 12 – lost in transcription. *Perspectives, studies in translatology*, 1-14. doi:10.1080/0907676X.2019.1708421
Messner, S. F., & Rosenfeld, R. (2013). *Crime and the American dream* (5 ed.). Belmont: Wadsworth.
Mills, C. W. (1940). Situated actions and vocabularies of motive. *American Sociological Review, 5*(6), 10.
Mistek, E., Fikiet, M. A., Khandasammy, S. R., & Lednev, I. K. (2019). Toward Locard's Exchange Principle: Recent developments in forensic trace evidence analysis.

Analytical chemistry (Washington), 91(1), 637-654. doi:10.1021/acs.analchem.8b04704
Mohliver, A. (2018). How misconduct spreads: Auditors' role in the diffusion of stock-option backdating. *Administrative Science Quarterly, 64*(2), 310-336. doi:10.1177/0001839218763595
Monk, J. K., Kanter, J. B., Jamison, T. B., & Russell, L. T. (2020). Beyond cold feet: Experiences of ending engagements and cancelling weddings. *Journal of social and personal relationships, 37*(12), 2921-2940. doi:10.1177/0265407520942590
Morales, J., Gendron, Y., & Guenin-Paracini, H. (2014). The construction of the risky individual and vigilant organization: A genealogy of the Fraud Triangle. *Accounting, Organizations and Society, 39*(3), 170-194.
Morse, J., & Richards, L. (2002). *Readme first for a user's guide to qualitative methods*. Thousand Oaks, CA: SAGE.
Murphy, D. S., & Robinson, M. B. (2008). The maximizer: Clarifying Merton's theories of anomie and strain. *Theoretical Criminology, 12*(4), 501-521. doi:10.1177/1362480608097154
Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: Understanding and preventing fraud in organizations. *Journal of Business Ethics, 101*(4), 601-618.
Nanduri, J., Jia, Y., Oka, A., Beaver, J., & Liu, Y.-W. (2020). Microsoft uses machine learning and optimization to reduce e-commerce fraud. *Interfaces (Providence), 50*(1), 64-79. doi:10.1287/inte.2019.1017
Nash, R. M., Bouchard, M., & Malm, A. (2013). Investing in people: The role of social networks in the diffusion of a large-scale fraud. *Social Networks, 35*(4), 686-698. doi:10.1016/j.socnet.2013.06.005
Nguyen, T. H., & Pontell, H. N. (2010). Mortgage origination fraud and the global economic crisis: A criminological analysis. *Criminology & Public Policy, 9*(3), 591-612. doi:10.1111/j.1745-9133.2010.00653.x
Nieto-Gomez, R. (2016). Stigmergy at the edge: Adversarial stigmergy in the war on drugs. *Cognitive Systems Research, 38*, 31-40. doi:10.1016/j.cogsys.2015.12.005
Northcott, C. (2018). MI5's tradecraft before the First World War. *International Journal of Intelligence and CounterIntelligence, 31*(2), 289-311. doi:10.1080/08850607.2017.1375327
Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International journal of qualitative methods, 16*(1), 1-13. doi:10.1177/1609406917733847
NSW Land Registry Services. (2021). Registrar General's guidelines. Retrieved from https://rg-guidelines.nswlrs.com.au/land_dealings/dealings_involving/resumptions
Obstfeld, D., Brown, J., & Carlile, P. (2019). Orchestrating networks of innovation in a world of constant change. *People and Strategy, 42*(2), 28-34.
Omar, M., Nawawi, A., Saiful, A., & Salin, A. P. (2016). The causes, impact and prevention of employee fraud: A case study of an automative company. *Journal of Financial Crime, 23*(4), 1012-1027.
Ortega, R. (2006). The insider threat: When trusted assets go bad. *Electric Light & Power, 84*(4), 22-24. Retrieved from http://ezproxy.csu.edu.au/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=egs&AN=21993990&site=ehost-live
Padgett, S. (2014). *Profiling the fraudster: Removing the mask to prevent and detect fraud*. Hoboken, New Jersey: Wiley.

Pao, T.-I., Tzeng, L. Y., & Wang, K. C. (2014). Typhoons and opportunistic fraud: Claim patterns of automobile theft insurance in Taiwan: Typhoons and opportunistic fraud. *The Journal of risk and insurance, 81*(1), 91-112.

Patton, M. Q. (2002). *Qualitative research and evaluation method* (3 ed.). Thousand Oaks CA: Sage.

Peabody, Z. (2001). Family held hostage; 3 Get $24,000: Two people hold a supermarket manager's wife and child at their home until the manager gives the money to a third person at the store. In (pp. B-7). Los Angeles: Los Angeles Times.

Phillips, C. (2017). From 'Rogue Traders' to organized crime groups: Doorstep fraud of older adults. *The British Journal of Criminology, 57*(3), 608-626. doi:10.1093/bjc/azw011

Piaget, J. (1980). The constructivist approach: Recent studies in genetic epistemology. *Cahiers de la Fondation Archives Jean Piaget, 1*, 1-7.

Pontell, H. N. (2009). Identity theft: Bounded rationality, research, and policy. *Criminology & Public Policy, 8*(2), 263-270. doi:10.1111/j.1745-9133.2009.00564.x

Pontell, H. N. (2016). Theoretical, empirical, and policy implications of alternative definitions of White-Collar Crime: Trivializing the lunatic crime rate In S. R. Van Slyke, M. T. Benson, & F. T. Cullen (Eds.), *The Oxford handbook of White-Collar Crime*. Oxford: Oxford University Press.

Pontell, H. N., Black, W. K., & Geis, G. (2013). Too big to fail, too powerful to jail? On the absence of criminal prosecutions after the 2008 financial meltdown. *Crime, law, and social change, 61*(1), 1-13. doi:10.1007/s10611-013-9476-4

Pontell, H. N., & Geis, G. (2014). The trajectory of white-collar crime following the great economic mltdown. *Journal of Contemporary Criminal Justice, 30*(1), 70-82. doi:10.1177/1043986213509022

Pontell, H. N., Ghazi-Tehrani, A., & Chang, T. (2017). Economic crime and China's high-speed railway: A case study of the Wenzhou crash. *Asian journal of criminology, 12*(1), 1-22. doi:10.1007/s11417-016-9242-5

Prabowo, H. Y. (2012). A better credit card fraud prevention strategy for Indonesia. *Journal of Money Laundering Control, 15*(3), 28.

Ragatz, L. L., Fremouw, W., & Baker, E. (2012). The psychological profile of white-collar offenders: Demographics, criminal thinking, psychopathic traits, and psychopathology. *Criminal Justice and Behavior, 39*(7), 978-997. doi:10.1177/0093854812437846

Ramamoorti, S. (2008). The psychology and sociology of fraud: Integrating the behavioural sciences component into fraud and forensic accounting curricula. *Issues in Accounting Education, 23*(4), 521-533.

Ramamoorti, S., & Olsen, W. (2007). Fraud: The human factor. *Financial Executive, 23*(6), 53-55.

Rashid, F. Y. (2016). The advanced security techniques of criminal hackers. *JavaWorld*.

Reiss, A. J. (1986). Co-offenders influence on criminal careers. In A. Blumstein, J. Cohen, J. A. Roth, & C. A. Visher (Eds.), *Criminal careers and career criminals* (Vol. 11). Washington: National Academy Press.

Reiss, A. J. (1991). Advancing knowledge about co-offending: Results from a prospective longitudinal survey of London males. *Journal of Criminal Law and Criminology, 82*, 360-395.

Rendon, J. M., & Rendon, R. G. (2016). Procurement fraud in the US Department of Defense. *Managerial Auditing Journal, 31*(6/7), 748-767. doi:10.1108/MAJ-11-2015-1267

Renzetti, C. M., Curran, D. J., & Carr, P. J. (2003). *Theories of crime: A reader*. Boston: Allyn and Bacon.

Reppetto, T. J. (1974). *Residential crime*. Cambridge: Ballinger Pub Co.
Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding Routine Activity Theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216-238. doi:10.1177/0022427811425539
Riemer, S. H. (1941). Embezzlement: Pathological basis. *Journal of Criminal Law and Criminology, 32*(4), 411-423.
Riess, W. (2011). The Roman bandit (Latro) as criminal and outsider. In M. Peachin (Ed.), *Oxford Handbooks in Classics and Ancient History. The Oxford handbook of social relations in the Roman world* (Vol. 1). doi:10.1093/oxfordhb/9780195188004.013.0034
Robinson, M., & Rogers, J. (2018). Applying contextual Anomie and Strain Theory to recent acts of corporate deviance. *Journal of Theoretical & Philosophical Criminology, 10*(2), 71-92.
Roche, S. P., Wilson, T., & Pickett, J. T. (2019). Perceived control, severity, certainty, and emotional fear: Testing an expanded model of deterrence. *The journal of research in crime and delinquency, 57*(4), 002242781988824-002242781988531. doi:10.1177/0022427819888249
Rothschild, D. P., & Thorne, B. C. (1976). Criminal consumer fraud: A victim-oriented analysis. *Michigan Law Review, 74*(4), 48.
Ruhland, E. L., & Selzer, N. (2020). Gender differences in white-collar offending and supervision. *Criminal justice studies, 33*(1), 13-30. doi:10.1080/1478601X.2020.1709950
Rustiarini, N. W., T, S., Nurkholis, N., & Andayani, W. (2019). Why people commit public procurement fraud? The Fraud Diamond view. *Journal of public procurement, 19*(4), 345-362. doi:10.1108/JOPP-02-2019-0012
S135.4 Criminal Code Act, 135.4 C.F.R. (1995).
S192G Crimes Act, § 192G (1900).
Sakurai, Y., & Smith, R. G. (2003). Gambling as a motivation for the commission of financial crime. *Trends & Issues in Crime & Criminal Justice, 256*.
Schell-Busey, N., Rorie, M., & Simpson, S. S. (2020). PROTOCOL: Protocol for corporate crime deterrence: An updated systematic review. *Campbell systematic review, 16*(2), n/a. doi:10.1002/cl2.1090
Schnatterly, K. (2003). Increasing firm value through detection and prevention of white-collar crime. *Strategic Management Journal, 24*(7), 27. doi:10.1002/smj.330
Schroeder, K. B., Pepper, G. V., & Nettle, D. (2014). Local norms of cheating and the cultural evolution of crime and punishment: A study of two urban neighbourhoods. *PeerJ, 2*, e450. Retrieved from https://primo.csu.edu.au/discovery/fulldisplay?docid=doaj_soai_doaj_org_article_b4a4b251fdc44a01bac7d6d250c22999&context=PC&vid=61CSU_INST:61CSU&search_scope=MyInst_and_CI&tab=Everything&lang=en
Schuchter, A., & Levi, M. (2015). Beyond the Fraud Triangle: Swiss and Austrian elite fraudsters. *Accounting Forum, 39*(3), 176-187. doi:10.1016/j.accfor.2014.12.001
Secchi, D. (2011). *Extendable rationality: Understanding decision making in organisations*. Dordrecht: Springer.
Seda, L., & Tilt, C. A. (2020). Disclosure of fraud control information in annual reports as a means of discharging public accountability. *Journal of Financial Crime, ahead-of-print*(ahead-of-print). doi:10.1108/JFC-11-2019-0154
Selzer, A. (2006). Biometrics call centres: Cutting fraud and enhancing service. *Biometric technology today, 14*(10), 9-10. doi:10.1016/S0969-4765(06)70611-7

Siemens, G. (2004). Connectivism: a learning theory for the digital age. Retrieved from www.elearnspace.org/Articles/connectivism.htm
Silver, J. (2013). 'For the union makes us ... rich?': Preventing trade union corruption in law after the Health Services Union saga. *Deakin Law Review, 18*(1), 127-158. doi:10.21153/dlr2013vol18no1art60
Simon, H. A. (1959). Theories of decision-making in economics and behavioural science. *The American Economic Review, 49*(3), 30.
Simon, H. A. (1978). Rationality as process and as product of thought. *The American Economic Review, 68*(2), 16.
Sipsma, H. L., Canavan, M. E., Rogan, E., Taylor, L. A., Talbert-Slagle, K. M., & Bradley, E. H. (2017). Spending on social and public health services and its association with homicide in the USA: An ecological study. *BMJ Open, 7*(10), e016379. doi:10.1136/bmjopen-2017-016379
Skinner, B. F. (1931). The concept of the reflex in the description of behaviour. *Journal of General Psychology, 6*, 22-37. doi:10.1080/00221309.1931.9918416
Skinner, B. F. (1938). *The behaviour of organisms: An experimental analysis*. New York: Appleton-Century-Crofts.
Slovic, P., Fischhoff, B., & Lichtenstein, S. (1977). Behavioural Decision Theory. *Annual Review of Psychology, 28*(1), 1. Retrieved from http://ezproxy.csu.edu.au/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=pbh&AN=11267892&site=ehost-live
Smith, B. L., Roberts, P., & Damphousse, K. R. (2016). The terrorists' planning cycle: Patterns of pre-incident behaviour. In G. LaFree & J. D. Freilich (Eds.), *The handbook of the criminology of terrorism*.
Smith, G., Button, M., Johnston, L., & Frimpong, K. (2011). *Studying fraud as white-collar crime*: Palgrave MacMillan.
Smith, H. J., Pettigrew, T. F., Pippin, G. M., & Bialosiewicz, S. (2012). Relative deprivation: A theoretical and meta-analytic review. *Personality and social psychology review, 16*(3), 203-232. doi:10.1177/1088868311430825
Smith, R. G. (2002). White-collar crime. In A. Graycar & P. Grabosky (Eds.), *The Cambridge handbook of Australian criminology* Cambridge: Cambridge University Press.
Smith, R. G. (2013). Organised crime and public sector corruption: A crime script analysis of tactical displacement risks. *Trends & Issues in Crime & Criminal Justice*(444).
Smith, R. G. (2014). *Responding to organised crime through intervention in recruitment pathways*. Retrieved from Canberra: https://www.aic.gov.au/publications/tandi/tandi473
Smith, R. G. (2018). *Estimating the cost to Australian businesses of identity crime and misuse*. Retrieved from Canberra: https://www.aic.gov.au/publications/rr/rr15
Soheila, M., Ali, M. Y., & Damien, C. (2005). Australian corporate collapse: The case of HIH Insurance. *Journal of Financial Services Marketing, 9*(3), 249. doi:10.1057/palgrave.fsm.4770157
Sohoni, T., & Rorie, M. (2019). The whiteness of white-collar crime in the United States: Examining the role of race in a culture of elite white-collar offending. *Theoretical Criminology*, 136248061986431. doi:10.1177/1362480619864312
Soltani, B. (2014). The anatomy of corporate fraud: A comparative analysis of high profile American and European corporate scandals. *Journal of Business Ethics, 120*(2), 251-274. doi:10.1007/s10551-013-1660-z
Steinmetz, K. (2015). Craft(y)ness. *The British Journal of Criminology, 55*(1), 125-145. doi:10.1093/bjc/azu061

Stephenson-Burton, A. (1995). 'Through the looking-glass': Public images of white-collar crime. In D. Kidd-Hewitt & R. Osborne (Eds.), *Crime and the media: The post-modern spectacle*. London: Pluto Press.
Stevenson, A. (Ed.) (2007) Shorter Oxford english dictionary. Oxford: Oxford University Press.
Stotland, E. (1977). White-collar criminals. *Journal of Social Issues, 33*(4), 179-196. doi:10.1111/j.1540-4560.1977.tb02531.x
Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing Grounded Theory*. Thousand Oaks, CA: Sage.
Suh, I., Sweeney, J., Linke, K., & Wall, J. (2020). Boiling the frog slowly: The immersion of c-suite financial executives into fraud. *Journal of Business Ethics, 162*(3), 645-673. doi:10.1007/s10551-018-3982-3
Sutherland, E. H. (1924). *Criminology* (2nd ed.). Philadelphia: Lippincott.
Sutherland, E. H. (1933). *Principles of criminology* (2nd ed.). Philadelphia: Lippincott.
Sutherland, E. H. (1939). *Principles of criminology* (3rd ed.). Philadelphia: Lippincott.
Sutherland, E. H. (1941). Crime and business. *Annals of the American Academy of Political and Social Science, 217*, 112-118. doi:10.2307/1023421
Sutherland, E. H. (1947). A theory of criminology. In *Principles of criminology* (4th ed., pp. 1-9). Philadelphia: Lippincott.
Sutherland, E. H. (1949). *White-collar crime*. New York: Dryden Press.
Sutherland, E. H. (1973). *On analyzing crime*. Chicago: University of Chicago Press.
Sutherland, E. H., & Cressey, D. R. (1974). *Criminology* (9th ed.). New York: Lippincott.
Swanborn, P. (2010). *Case study research: What, why and how?*
Sykes, G. M., & Matza, D. (1957). Techniques of neutralisation: A Theory of Delinquency. *American Sociological Review, 22*(6), 664-670. doi:10.2307/2089195
Tay, L.-M., Puah, C.-H., Brahmana, R. K., & Malek, N. I. A. (2016). The effect of white-collar crime announcement on stock price performance: Evidence from Malaysian stock market. *Journal of Financial Crime, 23*(4), 1126-1139. doi:10.1108/JFC-03-2015-0016
Taylor, E. (2013). Honour among thieves? How morality and rationality influence the decision-making processes of convicted domestic burglars. *Criminology and Criminal Justice*. doi:10.1177/1748895813505232
The Labour Party. (2019). *It's time for a real change: The Labour Party manifesto 2019*. London: The Labour Party
Topalli, V., Dickinson, T., & Jacques, S. (2020). Learning from criminals: Active offender research for criminology. *Annual review of criminology, 3*(1), 189-215. doi:10.1146/annurev-criminol-032317-092005
Tremblay, P. (1993). Searching for suitable co-offenders. In R. V. Clark & M. Felson (Eds.), *Routine activity and rational choice: Advances in criminological theory* (Vol. 5, pp. 17-36). New Brunswick: Transaction Books.
Trochim, W. M. K. (2021). Research methods knowledge base. Retrieved from https://conjointly.com/kb/nonprobability-sampling/
Tsai, C.-H., & Su, P.-C. (2021). The application of multi-server authentication scheme in internet banking transaction environments. *Information systems and e-business management, 19*(1), 77-105. doi:10.1007/s10257-020-00481-5
Tunley, M. (2010). Need, greed or opportunity?: An examination of who commits benefit fraud and why they do it. *Security Journal, 24*(4), 302. doi:10.1057/sj.2010.5
Turner, R. (2020). *Teenage kicks: The differential development of drug use, drunkenness, and criminal behaviour in early to mid-adolescence.* University of Gothenburg, Gothenburg.

Valukas, A. R. (2010). *Lehman Brothers Holdings Inc. Chapter 11 proceedings examiner's report*. Retrieved from New York: https://web.stanford.edu/~jbulow/Lehmandocs/menu.html
van den Broeke, L. (2015, 6 March 2015). Card-skimming gang targets banks' ATMs. *The Daily Telegraph*.
Van Koppen, P. J., & Jansen, R. W. J. (1998). The road to the robbery: Travel patterns in commercial robberies. *The British Journal of Criminology, 38*(Spring), 230-246. doi:10.1093/oxfordjournals.bjc.a014233
Van Nguyen, T. (2021). The modus operandi of transnational computer fraud: A crime script analysis in Vietnam. *Trends in Organized Crime*. doi:10.1007/s12117-021-09422-1
Vandeviver, C., Van Daele, S., & Vander Beken, T. (2015). What makes long crime trips worth undertaking? Balancing costs and benefits in burglars' journey to crime. *The British Journal of Criminology, 55*(2), 399-420. doi:10.1093/bjc/azu078
Vona, L. W. (2008). *Fraud risk assessment: Building a fraud audit program*. Hoboken NJ: John Wiley and Sons.
Vona, L. W. (2011). *The fraud audit responding to the risk of fraud in core business systems* (1st edition ed.). Hoboken, New Jersey: John Wiley & Sons.
Walsh, D. (2014). Victim selection procedures among economic criminals: The rational choice perspective. In D. B. Cornish & R. V. Clark (Eds.), *The reasoning criminal: Rational choice perspectives on offending*. New Brunswick: Transaction Publishers.
Walsh, L. (2012). Ounce of prevention, pound of cure *Research News*.
Walton, R. (2006). Balancing the insider and outsider threat. *Computer Fraud & Security, 2006*(11), 8-11. doi:10.1016/S1361-3723(06)70440-7
Wang, J., Gupta, M., & Rao, H. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly, 39*(1), 91. doi:10.25300/MISQ/2015/39.1.05
Warr, M. (1996). Organization and instigation in delinquent groups. *Criminology, 34*, 11-37. doi:10.1111/j.1745-9125.1996.tb01193.x
Watkins, D., & Gioia, D. (2015). *Mixed-method research*. doi:10.1093/acprof:oso/9780199747450.001.0001
Webber, C. (2007). Revaluating Relative Deprivation Theory. *Theoretical Criminology, 11*(1), 97-120. doi:10.1177/1362480607072737
Weerman, F. M. (2003). Co-offending as social exchange explaining: Explaining characteristics of co-offending. *The British Journal of Criminology, 43*(2), 398-416. doi:10.1093/bjc/43.2.398
Weisburd, D., Wheeler, S., Waring, E., & Bode, N. (1991). *Crimes of the middle classes: White-collar offenders in the federal courts*. New Haven: Yale University Press.
Weld, K. A. (2012). Dignifying the guerrillero, not the assassin: Rewriting a history of criminal subversion in postwar Guatemala. *Radical history review, 2012*(113), 35-54. doi:10.1215/01636545-1504885
Wells, J. T. (1997). *Occupational fraud and abuse: How to prevent and detect asset misappropriation, corruption and fraudulent statements*. Austin: Obsidian Publishing Company.
Wheeler, S., Weisburd, D., & Bode, N. (1982). Sentencing the white-collar offender: Rhetoric and reality. *American Sociological Review, 47*(5), 641-659. doi:10.2307/2095164
Wheeler, S., Weisburd, D., Waring, E., & Bode, N. (1988). White-collar crime and criminals. *American Criminal Law Review, 25*, 29.
White, R., & Perrone, S. (2015). *Crime, criminality & criminal justice*. Melbourne: Oxford University Press.

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of Routine Activities Theory. *Deviant Behavior, 40*(9), 1119-1131. doi:10.1080/01639625.2018.1461786

Williamson, G. R. (2003). Misrepresenting random sampling? A systematic review of research papers in the Journal of Advanced Nursing. *Journal of advanced nursing, 44*(3), 278-288. doi:10.1046/j.1365-2648.2003.02803.x

Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the four elements of fraud. *CPA Journal, 74*(12), 38-42. Retrieved from http://ezproxy.csu.edu.au/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=15290416&site=ehost-live

Wood, T., & da Costa, A. P. P. (2015). Corporate frauds as criminal business models: An exploratory study. *Thunderbird International Business Review, 57*(1), 51-62. doi:10.1002/tie.21676

Wuth, R. (2015, 26 February 2015). Card skim gear seized. *Gold Coast Bulletin*.

Yates, J. (2003). The Crime and Disorder Act 1998: Implications for youth justice in England and Wales. *Kriminologija & Socijalna Integracija, 11*(1), 49.

Yin, R. K. (2014). *Case study research: Design and methods*. Thousand Oaks CA: Sage Publications.

Young, J. (1981). Thinking seriously about crime: Some models of criminology. In M. Fitzgerald, G. McLennan, & J. Pawson (Eds.), *Crime and society: Readings in history and society* (pp. 248-309).

Yusof, N. A. M., & Lai, M. L. (2014). An integrative model in predicting corporate tax fraud. *Journal of Financial Crime, 21*(4), 424-432. doi:10.1108/JFC-03-2013-0012

Zafirovski, M. (2018). Rational Choice Theory or pretense? The claims, equivalences, and analogies of the "economic approach to human behaviour". *Sociological Spectrum, 38*(3), 194-222. doi:10.1080/02732173.2018.1469446

Zembroski, D. (2011). Sociological theories of crime and delinquency. *Journal of Human Behaviour in the Social Environment, 21*(3), 240-254. doi:10.1080/10911359.2011.564553

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by knowledge exchange behaviours. *Information Systems Frontiers, 17*(6), 1239-1251. doi:10.1007/s10796-015-9567-0

Zimring, F. E. (1981). Kids, groups and crime: Some implications of a well-known secret. *Journal of Criminal Law and Criminology, 3*, 867-885. doi:10.2307/1143269

Appendices

Appendix A: Participant Selection Criteria

This document, linked to Protocol 2014/564, contains the criteria used to select research participants.

Participants will be drawn from either the Australian Federal Police or the New South Wales Police Force.

For a participant to take part in this research they must meet the following criteria:

1. They must either hold an investigative post, or have previously held an investigative post within the past three years within the Australian Federal Police, or the New South Wales Police Force.
2. They must be or have been, an Officer in Charge (OIC) of a Fraud Investigation while with the Australian Federal Police or the New South Wales Police Force.
3. They must have been an OIC for at least one case that has been finalised in an Australian Court of Law.

Appendix B: Participant Information Sheet

This document, linked to Protocol 2014/564, contains the information provided to participants ahead of their involvement in the semi-structured interviews.

Researcher:

My name is Douglas Allan, I am a doctoral candidate at the Criminology Department within the School of Sociology at the Australian National University.

I have a professional background that includes policing and public and private sector investigations experience from New Zealand, Scotland, and England. I have worked with the European Anti-Fraud Office, the Nigerian Economic and Financial Crimes Commissions and the Scottish and English NHS Counter Fraud Services. I am employed as a lecturer of Law Enforcement and teach investigations, foundations in financial crime and fraud and financial crime risk management at the Australian Graduate School of Policing and Security, and the School of Policing with Charles Sturt University. I am completing this research in my role as a doctoral candidate at the Australian National University.

Project title:

Fraud and Financial Crime: unpacking offender approaches to complex financial systems

Project description:

- General description and methodology

This project aims to explain how fraudsters overcome anti-fraud systems sited in complex financial systems. The project uses case management files held by the New South Wales Police Fraud Squad, Official Court Transcripts held by the NSW Courts Services and interviews with individuals involved in the commission of eight frauds and the investigation and prosecution of those eight frauds. The project is split into three phases; phase one (to which this Participant Information Sheet relates) involves interviews with NSWPF detectives,

phase two involves the thematic examination of eight fraud cases, phase three involves interviews with, yet unknown, individuals who have relative proximity to, and understanding of the eight cases.

- Participants

As a participant in phase one of this research, I will collect data from you by way of a semi-structured interview. I will be interviewing between six and ten NSWPF detectives to identify eight complex fraud cases. Analysis of the eight fraud cases will identify between eight and 16 further participants based on their relative proximity to, and understanding of, the eight cases.

- Use of data and feedback

The data obtained during the case analysis and interviews will be used to help explain how fraudsters overcome anti-fraud systems found within complex financial systems. Data derived from this research will be used in a thesis, publications and potentially in future research. As a research participant, you will automatically receive feedback in the form of a summary of the research.

Participant involvement:

- Voluntary participation and withdrawal

Participation in this research is entirely voluntary. You are free to decline to take part or withdraw from the research, at any time, without explaining up until the research is prepared for publication. There are no penalties should you choose to withdraw from this research. If you withdraw from the research the data, you have supplied with be securely destroyed. Alternatively, should you consent, your data may continue to be used after you have withdrawn from the research.

- What will participants be expected to do

If you agree to participate in this research, you will engage in a semi-structured interview with me. Should you agree to the interview, you may refuse to answer any question/s or stop the interview at any time without explaining. I intend to make an audio recording of this interview, but this will only occur with your express consent. If you consent to this interview being audio-recorded, only my principal research supervisor and I will have access to it. If you wish to receive a transcript of your interview, that will be provided before the finalisation of its analysis. The semi-structured interviews in phase one will focus on the following areas: 1) Individual knowledge and professional experience, 2) Role of a Fraud Squad detective, and 3) Identification of case studies.

- Location and duration

The interview will take place, face to face, in a location suitable to you. Most likely it will take place within the NSWPF State Crime Command building in Paramatta. It is anticipated interviews will take approximately 90 minutes; however, you are free to refuse to answer a question/s or stop the interview at any time without explaining. While you may be asked to take part in a follow-up interview, you are free to decline.

- Risks

It is anticipated there will be limited risks in phase one of the research, however, all efforts will be made to ensure that there are no discomforts, hazards, or side effects due to your involvement in this project.

Exclusion criteria:

You will be excluded from this research if you do not meet the following listed criteria:

1. You must either hold an investigative post or have previously held an investigative post within the past three years within the NSWPF Fraud Squad;

2. You must be, or have been, an Officer in Charge (OIC) of a Fraud Investigation while with the NSWPF Fraud Squad;
3. You must have been an OIC for at least one case that has been finalised in a Court of Law.

Confidentiality:

By participating in an interview, you agree (via signing a Written Consent Form) for me to collect and store data obtained from the interview to conduct this research project. The data you provide in the interview will be de-identified and coded. Your details including the Written Consent Form and code references linking you to your data will be held separately from the data you provide in the interview so you can not be identified directly from the interview data.

I will become the custodian of the data you provide during the interview, but the data remains yours. The only people that will have access to your data will be my principal research supervisor and I will ensure confidentiality will be preserved as far as allowed by law.

Data storage:

It is anticipated that most data obtained will be in an electronic form. Electronic data generated during this project will be stored on a password protected FIPS 140-2 Level 3 Military Grade Encryption Kingston 6000 USB device. To ensure confidentiality I will de-identify all data so you and your data will only be referred to by code. Code references linking you to your data will be stored separately on a second password protected Encrypted Kingston 6000 USB device. Written Consent Forms and any other written materials will be stored at the NSWPF Academy in locked document storage safe to which only I have access. All data will be stored for at least five years following publication.

Queries and concerns:

Should you have any questions about this research project, please direct your queries to either me or, especially if you have any concerns or questions about my research or my conduct as I carry out this research please direct them to either Professor Roderic Broadhurst, my principal research supervisor, or Dr Christopher Devery, my co-supervisor and Principal Research Officer for the NSWPF.

Douglas Allan
PhD Candidate

Department of Criminology
|School of Sociology |
College of Arts and Social Sciences |Australian National University

Berryl Rawson Building #13
13 Ellery Crescent
The Australian National University, Canberra, ACT, 2601
T:
E:

Professor Roderic Broadhurst
Principal Supervisor

Department of Criminology
|School of Sociology |
College of Arts and Social Sciences |Australian National University

Berryl Rawson Building (#13)
13 Ellery Crescent
The Australian National University, Canberra, ACT, 2601

T:
E:

Dr Christopher Devery
Co-supervisor at NSWPF

NSWPF Research Office

NSW Police Academy
McDermott Drive,
Goulburn, NSW, 2580

T:
E:

Ethics Committee Clearance:

The ethical aspects of this research have been approved by the ANU Human Research Ethics Committee. If you have any concerns or complaints about how this research has been conducted, please contact:

Ethics Manager

The ANU Human Research Ethics Committee

The Australian National University

T:

E:

Appendix C: Written Consent Form

This document, linked to Protocol 2014/564, is the written consent form that participants read and signed before engaging in the semi-structured interview.

Project title:

Fraud and Financial Crime: unpacking offender approaches to complex financial systems

Participation:

I have read and understood the Information Sheet you have given me about the research project, and I have had any questions and concerns about the project addressed to my satisfaction.

YES ☐ NO☐ I agree to participate in the project.

YES ☐ NO ☐ I agree to this interview being audio-recorded

Data collection, storage, and future use:

I consent for the principal investigator to collect and store data obtained from this interview to conduct the above research project. I understand that all data will be de-identified at the data collection stage for data storage.

I understand that before any data collected during this interview is published, I will be contacted to seek second permission to allow this. Data will only be used upon obtaining this second permission.

Consent:

Name: ……. Signature: ……

Appendix D: Letter to Participants

This document, linked to Protocol 2014/564, is the initial letter sent to individual participants inviting them to take part in the study.

NSWPF Fraud & Cybercrime Squad

State Crime Command,

New South Wales Police Force

1 Charles Street

Paramatta, 2150

NSW

Friday, 17th October 2014

Fraud Squad Investigator

Doctoral Research Proposal – Fraud and Financial Crime: unpacking offender approaches to complex financial systems

My name is Douglas Allan; I am a doctoral candidate at the Criminology Department in the School of Sociology at the Australian National University. My doctoral study examines how fraudsters overcome anti-fraud systems sited in complex financial systems. To facilitate this research, I am seeking to interview members of the NSWPF Fraud & Cybercrime Squad. This research has been approved by Dr Chris Devery, manager of the NSWPF Research Coordination Unit.

If you agree to participate in this research, you will be engaged in a semi-structured interview. It is anticipated the interview will take no longer than 50 minutes and will take place at the NSW Police Force Headquarters, or another location of your choice. Participation in this research is voluntary.

If you would like more information about the research or would like to participate in the research, please advise me via email at [email removed at the time of submission].

Appendix E: Interview Questions

This document, linked to Protocol 2014/564, contains the questions that were used during the semi-structured interviews with the research participants.

Individual knowledge and professional experience:

1. How long have you been a Police Officer?
2. How long have you worked on complex fraud cases?
3. What generic knowledge or expertise did you possess before joining the Fraud Squad that aids in the understanding and investigation of complex frauds?
4. What specific knowledge or expertise did you possess before joining the Fraud Squad that aids in the understanding and investigation of complex frauds?
5. What training/development have you undertaken since joining the Fraud Squad?
6. What training/development would you deem necessary to undertake before, or having commenced service with the Fraud Squad?
7. How many cases have you been OIC for since joining the Fraud Squad?
8. How many cases have you assisted with since joining the Fraud Squad?

About the role:

9. Tell me about your role as a Fraud Squad detective?
10. I will shortly provide you with a range of prompt words or phrases that are designed to elicit a descriptive response from you about the types of cases you investigate. When I supply the prompt word, please describe the characteristics of cases you are familiar with:
    a. Victim characteristics
    b. Offender characteristics
    c. Types of organisations
    d. Types of financial systems

e. The complexity of financial systems

f. Anti-Fraud Controls (AFC) present

g. Complexity of crimes

h. How offenders committed their crimes

i. Evidence of Planning

j. Preparatory actions leading up to the crime

k. Post-crime actions

l. Planned or opportunity

m. Motivation

n. Value of fraud

o. Access to financial systems

p. Employee or external actor

Identification of Case Studies:

11. Having regard to the areas we have just discussed; can you please identify three cases you have been involved in that meet the following criteria:

a. The fraud occurred within a definable financial system; and which is

b. Suitably complex; and

c. Where the fraud required more than mere deception on the part of one individual: and

d. Is valued over $10,000 AUD; and/or

e. Was committed across multiple jurisdictional boundaries; and

f. Required the presence of an employee/ internal actor for the crime to occur.

Deliberately excluded from this typology are fraud cases:

a. That is not situated within an organisational/governmental setting; or

b. Where the offence and subsequent investigation was primarily conducted outside of NSW.

Specifics on offending: (repeat for each case presented)

12. Having identified three cases, I would now like to explore each case in turn with you in a little more detail from your perspective.

As you know I am interested in the planning carried out by fraudsters and in the decisions, they make when faced with anti-fraud controls within complex financial systems. As such I would like to hand it over to you to understand how they plan and why they make the decisions they do from your perspective.

13. Finally, I have some final questions that I would like to ask to wrap up this case:

    a. How important was it for the criminal in this case to understand the workings of the financial system and why?
    b. Describe how the offender/s gained that knowledge.
    c. What motivations were present in this crime?
    d. At what stage were these motivations formed?
    e. Describe the extent of anti-fraud controls present within the financial system.
    f. Describe the part of the system that was targeted by the offender.
    g. What weaknesses were present within the system?
    h. Why did that weakness occur?
    i. How was the offender able to identify that weakness?
    j. What influenced the offender in their selection?
    k. Describe the extent of anti-fraud controls present within the specific part of the financial system targeted by the offender?
    l. Describe the actions of the offender to overcome the relevant anti-fraud system.

Appendix F: Case Selection Criteria

This document, linked to Protocol 2014/728, contains the criteria upon which case man agent files were selected.

The fraud occurred within a definable financial system; and which is

a. Suitably complex; and
b. Where the fraud required more than mere deception on the part of one individual: and
c. Is valued over $10,000 AUD; and/or
d. Was committed across multiple jurisdictional boundaries, and
e. Required the presence of an employee/ internal actor for the crime to occur.
f. Deliberately excluded from this are fraud cases: That is not situated within an organisational/governmental setting; or where the offence and subsequent investigation was primarily conducted outside of NSW of the jurisdiction of the Australian Federal Police.