



Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Play Your Cards Right

Preventing Criminal Abuse of Online Gambling

Anton Moiseienko



Play Your Cards Right

Preventing Criminal Abuse of Online Gambling

Anton Moiseienko

RUSI Occasional Paper, November 2019



Royal United Services Institute
for Defence and Security Studies

188 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

The views expressed in this publication are those of the author, and do not reflect the views of RUSI or any other institution.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <<http://creativecommons.org/licenses/by-nc-nd/4.0/>>.

RUSI Occasional Paper, September 2019. ISSN 2397-0286.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Acknowledgements	v
Executive Summary	vii
Introduction	1
I. AML/CTF Regulation of Online Gambling	3
Rationale for AML/CTF Regulation	3
Scope of AML/CTF Regulation	6
II. Risks and Mitigation	11
Operator-Related Risks	11
Customer-Related Risks	14
III. Interaction with Financial Institutions	23
The Importance of Payment Processing	23
Transaction Laundering	24
Effects of Uncertainty	24
IV. Interaction with Law Enforcement	27
Conclusions and Recommendations	29
About the Author	33

Acknowledgements

This paper forms part of the Financial Crime 2.0 research programme funded by EY and Refinitiv. The author would like to thank James Banks, Sine Edal, Tom Keatinge and an anonymous reviewer for their helpful comments on an earlier version of this paper, and owes its title to Isabella Chase.

Thanks are also due to all those who have generously offered their time to be interviewed for this research or who took part in the workshop, as well as the RUSI publications team for their characteristically excellent editing.

Executive Summary

FOR A WELL-STUDIED subject, a remarkable diversity of opinion exists on the financial-crime risks of online gambling. In 2019, the EU's supranational risk assessment assigned the online gambling sector its second-highest risk rating and cited 'huge' volumes of transactions as a key reason for its potential appeal to money launderers.¹ In contrast, the National Risk Assessment in the UK, which is the world's largest regulated online gambling market by revenue,² has consistently ranked online gambling-related risks as 'low', although the assessment's methodology section underscores that money laundering can also happen through 'low-risk' sectors.³

This is not simply a divide between European and British attitudes, however. A survey of 204 compliance, finance and legal executives in the UK in 2019 suggested gambling is the sector most often seen as at risk of money laundering.⁴ And yet, in the UK and elsewhere, confirmed instances of money laundering through online gambling remain few and far between, with the exception of organised crime infiltration.⁵ Amidst these conflicting indicators, one wonders whether a decade-old assessment that online gambling offers only 'modest' opportunities for financial crime still holds true today.⁶

Based on a workshop held in London in May 2019, a series of interviews and a review of public sources, this paper explores money-laundering and terrorist-financing risks faced by online gambling operators and recommends measures for their mitigation. This research draws both on the UK experience and interviews with representatives of four other European countries' domestic authorities. Given the cross-border nature of online gambling, this paper's findings and recommendations are intended to be of use in both the UK and other countries that regulate online gambling (rather than prohibit it outright).

-
1. European Commission, 'Commission Staff Working Document Accompanying the Document Report from the Commission to the European Parliament and the Council on the Assessment of the Risk of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-Border Activities', 24 July 2019, SWD (2019) 650 final, p. 223.
 2. Gambling Commission, 'Review of Online Gambling', March 2018, p. 9.
 3. HM Treasury and Home Office, *National Risk Assessment of Money Laundering and Terrorist Financing 2017* (London: The Stationery Office, 2017), p. 76. For a description of methodology, see pp. 83–84.
 4. LexisNexis Risk Solutions and Economist Intelligence Unit, 'On the Frontline: The UK's Fight Against Money Laundering', 2019, p. 8.
 5. Europol, 'From Suspicion to Action: Converting Financial Intelligence into Greater Operational Impact', 2017, p. 14.
 6. Michael Levi, 'Money-Laundering Risks and E-Gaming: A European Overview and Assessment', European Gaming and Betting Association, September 2009, p. 6.

In line with earlier research,⁷ this paper finds that, like other businesses, online gambling faces some risk of criminal exploitation. At its simplest, it involves gambling of criminal proceeds for fun, rather than for cleansing illicit income. While it is inevitable that small illicit transactions can go under the radar of both gambling operators and financial institutions, gambling operators' customer due diligence (CDD) should contribute to the detection of anomalous behaviour. Apart from financial crime, atypical gambling patterns may signify problem gambling,⁸ which further elevates the importance of effective CDD measures.

At present, however, there is considerable variance in UK gambling operators' CDD practices, such as monetary thresholds for enhanced due diligence, and in approaches taken to one of the most widespread criminal typologies that the sector faces, namely the use of stolen bank cards. This paper's first recommendation is for gambling regulators to consider thematic reviews focused on CDD practices and the detection of stolen cards.

The second recommendation is for law enforcement agencies and/or financial intelligence units to conduct and publish analysis of typologies based on suspicious activity reports (SARs),⁹ which, for all their imperfections as a dataset, can offer a sector-wide perspective on financial crime risks that businesses think they face. As a recent review of 250 SARs related to UK land-based casinos demonstrates,¹⁰ this work can be a fruitful way of enhancing collective threat awareness.

Since customers need to make and receive payments to gamble, the remaining three recommendations concern the payments infrastructure underpinning online gambling. Specifically, they advocate:

- For those national regulators who have not yet done so, to inform financial institutions about unlicensed gambling operators that illegally offer services in the respective jurisdiction.
- For financial services regulators to review financial institutions' ability to detect transaction laundering, in other words concealing the real nature of one's business to obtain access to payment facilities.
- For governments to clarify which cryptocurrency activities online gambling operators can undertake and ensure their anti-money-laundering/counterterrorist-financing supervision by a regulator with adequate resources and expertise.

7. See *Ibid.*; Moneyval, 'The Use of Online Gambling for Money Laundering and the Financing of Terrorism Purposes: Research Report', April 2013.

8. That is, gambling that disrupts or damages personal, family or recreational pursuits. See Royal College of Psychiatrists, 'Problem Gambling', <<https://www.rcpsych.ac.uk/mental-health/problems-disorders/problem-gambling>>, accessed 28 August 2019.

9. Also referred to as suspicious transaction reports (STRs) or suspicious matter reports (SMRs), depending on the jurisdiction.

10. Graham Edwards, 'Suspicious Activity Reports (SARs) Analysis on the Criminal Use of the Gaming (Casino) Sector', *ACAMS Journal* (Vol. 1, No. 1, 2019), p. 34.

Introduction

GAMBLING IS NOT immune to criminal misuse.¹ Rightly or wrongly, the image of a high-rolling gangster is a fixture of popular culture. But beyond lifestyle spending (criminals gambling for fun) and criminal infiltration (criminals running gambling businesses), it remains uncertain how vulnerable the gambling industry is to money laundering.

On the one hand, certain regulators have taken extensive action against anti-money-laundering/counterterrorist-financing (AML/CTF) failings among gambling businesses, including Great Britain's Gambling Commission (Northern Ireland has a separate gambling regime).² Furthermore, a survey of 204 compliance, finance and legal executives in the UK in 2019 suggested that 15% of the respondents see gambling as the sector most at risk of money laundering.³ In 2018, two UK academics noted that among gambling-related crime, money laundering and terrorist financing⁴ had garnered the most attention.⁵ On the other hand, there is little publicly available evidence of criminals actually exploiting AML/CTF deficiencies of online gambling operators, let alone doing so at scale.

Against this background, the objective of this paper is to contribute to a better understanding of money-laundering and terrorist-financing risks faced by online gambling operators and measures for their mitigation.

The paper is based on: a literature review; a workshop convened by RUSI in London on 10 May 2019 with participation from online gambling operators, an industry group, a regulatory agency, a lawyer specialising in advising gambling companies, law enforcement agencies, and

-
1. This paper uses the term 'gambling'. Elsewhere, 'gaming' is often used as a synonym.
 2. The Gambling Commission's enforcement actions in relation to both companies and individuals are listed at Gambling Commission, 'Regulatory Action', <<https://www.gamblingcommission.gov.uk/news-action-and-statistics/Regulatory-action/Regulatory-action.aspx>>, accessed 28 August 2019.
 3. LexisNexis Risk Solutions and Economist Intelligence Unit, 'On the Frontline: The UK's Fight Against Money Laundering', 2019, p. 8. The report does not break the responses down by sectors, so it is unknown to what extent this perception is attributable to the views of those working in the gambling sector.
 4. Referred to as 'financial crime' for brevity in this paper.
 5. James Banks and Dan Waugh, 'A Taxonomy of Gambling-Related Crime', *International Gambling Studies* (Vol. 19, No. 2, 2019), p. 339.

academia; and 13 interviews with subject-matter experts⁶ and one written reply.⁷ In the case of interviews with regulators, their respective countries are not disclosed in keeping with the promise given to these interviewees to ensure the anonymity of the institutions involved. When possible, interviewee statements were verified against other publicly available information. Although some caution is necessary when relying on these statements, given the size of the interview sample, they provide helpful insight into the issues discussed in the paper.

Since the research was conducted in the UK, it mostly – but not exclusively – draws on the UK experience as well as interviews with representatives of four other European countries' domestic authorities. Given the cross-border nature of online gambling, this paper is intended to also be of use to readers in other countries that regulate online gambling (rather than prohibit it outright).

Following the introduction, the paper discusses, in turn:

- The AML/CTF regulation of online gambling.
- Financial crime risks of online gambling and measures taken to tackle them.
- The interaction of online gambling operators with financial institutions.
- The interaction of online gambling operators with law enforcement agencies.

6. Author interview with consultant A, London, 21 January 2019; author interview with consultant B, London, 22 January 2019; author interview with regulator A, European country, 13 February 2019; author interview with law enforcement officer A, European country, 1 March 2019; author interview with consultant C, London, 4 April 2019; author telephone interview with cryptocurrency compliance officer A, 4 April 2019; author interview with financial intelligence unit (FIU) officer A, European country, 16 May 2019; author telephone interview with academic A, 20 May 2019; author telephone interview with FIU officer B and regulator B, 7 June 2019; author telephone interview with regulator C, 17 June 2019; author interview with payment processing company A, London, 2 July 2019; author interview with non-UK law enforcement officer B, London, 29 August 2019; author interview with cryptocurrency compliance officer B (with prior experience of the gambling sector), London, 5 September 2019.

7. Written reply from FIU officer D, European country, 12 August 2019.

I. AML/CTF Regulation of Online Gambling

THIS CHAPTER CONSIDERS the AML/CTF regulation of online gambling, discussing why some online gambling businesses have been made subject to AML/CTF obligations, and which online gambling businesses are covered by such regulation.

Rationale for AML/CTF Regulation

Financial Footprint of Online Gambling

Developments in communication have seen a significant proportion of gambling move online. Online gambling (excluding lotteries) by customers in Great Britain, the world's largest regulated online gambling market, accounts for 34% (£4.7 billion) of the gambling industry's total gross gambling yield⁸ (£13.8 billion).⁹ It was reported that online gambling globally amounted to \$45.8 billion as of 2017.¹⁰

There is a concern that the amount of funds involved in online gambling can make the sector attractive to criminals seeking to disguise their illicit activity. For instance, the EU's supranational risk assessments in 2017 and 2019 deemed online gambling to pose 'significant' financial crime risks.¹¹ Table 1 summarises several risk assessments relevant to major European gambling jurisdictions.

8. Gambling operator's income minus payouts to players.

9. Gambling Commission, 'Review of Online Gambling', March 2018, p. 9.

10. Zion Market Research, 'Global Online Gambling & Betting Market Will Reach USD 94.4 Billion by 2024', 19 September 2018, <<https://www.globenewswire.com/news-release/2018/09/19/1572852/0/en/Global-Online-Gambling-Betting-Market-Will-Reach-USD-94-4-Billion-By-2024-Zion-Market-Research.html>>, accessed 28 August 2019.

11. European Commission, 'Report from the Commission to the European Parliament and the Council on the Assessment of the Risk of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-Border Activities', 26 June 2017, COM(2017) 340 final, p. 5; European Commission, 'Report from the Commission to the European Parliament and the Council on the Assessment of the Risk of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-Border Activities', 24 July 2019, COM(2019) 370 final, p. 4.

Table 1: Selected Risk Assessments of Online Gambling

Jurisdiction	Year	Risk	Rationale
European Commission (EU)	2019	'Significant' (3/4)	The European Commission cites 'huge' transactional volumes and notes that only a 'moderate level of expertise' is required of a would-be launderer.
	2017	'Significant' (3/4)	
Gambling Commission (UK)	2019	'High' (4/5)	The assessment contains a detailed review of risks pertaining to operator control, licensing and integrity, customer, products and means of payment. The 'high' rating is an overall assessment of risk in both online casinos and other online gambling businesses.
	2018	'Higher' (3/3)	
Home Office and HM Treasury (UK)	2017	'Low' (1/3)	The assessment noted the 'continued lack of evidence of the use of the sector for money laundering on a significant scale', as well as lack of evidence of its abuse for terrorist financing.
	2015	'Low' (1/3)	
Gambling AML Group (UK)	2017	N/A	The assessment lists various risk factors before and after mitigation measures are taken, but does not contain an overall risk score.
Isle of Man	2015	'Medium' (3/5)	The sector's vulnerabilities are assessed as 'medium' and the overall effectiveness of mitigation measures as 'medium high'. Moneyval's 2016 evaluation found this assessment reasonable and noted that gambling was the largest sector of the island's economy, contributing 16.7% of its GDP.
Gibraltar	2018	5/8 for money laundering 2/8 for terrorist financing	Despite the relatively high threat score, the assessment notes that most transactions are low-volume and states that 'the threat ... is in large part mitigated by the fact that transactions are so carefully recorded and monitored'.
Malta	2018	'Low' (1/4)	Gambling contributes 12% of Malta's GDP. In relation to online gambling, the assessment merely states that the sector became regulated in 2018 and the Maltese Gaming Agency began conducting AML/CTF inspections then.
Moneyval	2013	N/A	The report listed a range of possible vulnerabilities but did not rate the risks.

Sources: European Commission, 'Commission Staff Working Document', p. 223; Gambling Commission, 'Money Laundering and Terrorist Financing Risk Within the British Gambling Industry', June 2019, pp. 42, 52; HM Treasury and Home Office, National Risk Assessment of Money Laundering and Terrorist Financing 2017 (London: The Stationery Office, 2017), p. 76; Gambling Anti-Money Laundering Group (GAMLG), 'GAMLG's AML Risk Assessment for Licensed Betting Offices (LBOs) and Remote Gambling Industries', 2016, pp. 11–14; Moneyval, 'Anti-Money Laundering and Counter-Terrorist Financing Measures Isle of Man: Fifth Round Mutual Evaluation Report', December 2016, pp. 6, 16–17; HM Government of Gibraltar, '2018 National Risk Assessment: Money Laundering and Terrorist Financing Risks', September 2018, pp. 22–23; Republic of Malta, 'Results of the ML/TF National Risk Assessment', 2018, pp. 10, 18; FATF and Asia/Pacific Group on Money Laundering,

'Vulnerabilities of Casinos and Gaming Sector', March 2009; Moneyval, 'The Use of Online Gambling for Money Laundering and the Financing of Terrorism Purposes: Research Report', April 2013.

Note: Only the rationale for the most recent risk assessment is provided in Table 1. Note that FATF and Asia/Pacific Group on Money Laundering, 'Vulnerabilities of Casinos and Gaming Sector' did not consider online gambling.

The Dutch Financial Intelligence Unit (FIU) reportedly conducted a risk assessment of online gambling in 2014 in anticipation of the legalisation of online gambling, but it is not publicly available.¹² A brief paper commissioned in 2017 by the Dutch Ministry of Security and Justice assessed risks of online gambling as 'high', but only considered illegal online gambling.¹³

Differences Between Online and Land-Based Gambling

Although the financial footprint of land-based gambling is no smaller, online gambling poses distinct challenges for various stakeholders, namely:

- **Online gambling operators** must contend with a wider array of financial-crime risks posed by non-face-to-face customer interaction, higher-risk jurisdictions and various types of criminal proceeds, such as potential use of stolen bank cards. A research paper published in 2013 suggested that money-laundering opportunities in online gambling might be 'unique' due to a combination of eight factors, including the industry's cross-border nature, a large number of legal and illegal operators, and complexity of payment processing.¹⁴ On the other hand, online gambling operators can track and analyse their customers' activities in a way that land-based operators cannot.
- **Regulators** in charge of online gambling operators need to regulate and supervise businesses that, depending on the country's regulatory regime, may be located beyond its borders.¹⁵

12. Killian McCarthy, 'Money Laundering Prevention in Online Gambling in the Netherlands', in Ingo Fiedler et al., *Das Geldwäscherisiko verschiedener Glücksspielarten* (Wiesbaden: SpringerGabler, 2017), p. 114.

13. J van der Knoop, 'Risks of Money Laundering and the Financing of Terrorism in the Gambling Sector: Quick Scan', Research and Documentation Centre WODC (Wetenschappelijk Onderzoek – en Documentatiecentrum) of the Dutch Ministry of Security and Justice, 2 April 2017, p. 4, <https://www.wodc.nl/binaries/2689F_Summary_tcm28-253480.pdf>, accessed 28 August 2019.

14. Ingo Fiedler, 'Online Gambling as a Game Changer to Money Laundering?', 28 May 2013, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2261266>, accessed 28 August 2019.

15. The functions of AML/CTF regulation (making the rules) and supervision (monitoring compliance) can be separate and carried out by distinct agencies, but this is rare in the gambling context (for instance, see the list of European gambling regulators at Gaming Regulators European Forum, <<http://www.gref.net/regulators-in-europe/>>, accessed 8 October 2019). This paper assumes that 'regulators' carry out both regulation and supervision.

- **Law enforcement agencies** (LEAs) need to detect, investigate and prosecute online gambling-related misconduct that may involve perpetrators and assets across a variety of countries.

In addition to these general risks, there are financial crime vulnerabilities specific to particular types of gambling services. As with land-based gambling, services provided by online gambling operators can include casino games (such as roulette),¹⁶ betting (such as on an outcome of a sports event), card games (such as poker), and other games of chance (such as bingo). In peer-to-peer games, such as online poker, a user can intentionally 'lose' to another customer to transfer value, which may derive from criminal proceeds.¹⁷ This method could be used to pay for illicit goods or simply move funds.¹⁸ Meanwhile, betting sites could be used to monetise match-fixing and thus generate criminal proceeds, which can sometimes be detected by identifying atypical betting behaviour.¹⁹ In this connection, it is worth noting that a report in 2014 alleged that \$140 billion annually was laundered through sports betting, but did not explain the provenance of the figure.²⁰

Scope of AML/CTF Regulation

Regulation of Casinos

Some states prohibit or criminalise gambling, including online gambling, while others subject it to regulation.²¹ If online gambling takes place in a state where it is criminalised, handling its proceeds constitutes money laundering from that state's standpoint.²²

16. The UK's legal definition of a casino game is 'a game of chance which is not equal chance gaming': in other words, a customer plays against the bank and has less chance of winning than the bank. See 'Gambling Act 2005 (UK)', section 7(2).

17. Gambling Anti Money Laundering Group (GAMLG), 'GAMLG's AML Risk Assessment', p. 23.

18. Fiedler, 'Online Gambling as a Game Changer to Money Laundering?', p. 4. The point is reiterated in Charles McFarland, François Paget and Raj Samani, 'Jackpot! Money Laundering Through Online Gambling', McAfee Labs White Paper, 2013, p. 8.

19. Author interview with consultant C, London, 4 April 2019.

20. Université Paris 1 Panthéon-Sorbonne and the International Centre for Sport Security, 'Protecting the Integrity of Sport Competition', May 2014, p. 29.

21. A helpful overview is available at GamblingSites.com, 'Online Gambling Laws and Jurisdictions', <<https://www.gamblingsites.com/online-gambling-jurisdictions/>>, accessed 28 August 2019.

22. For instance, in 2013 the US Attorney for the Southern District of New York indicted 34 individuals for organising an illicit gambling ring catering to wealthy clientele and laundering its proceeds, see US vs. Tokhtakhounov et al., Sealed Indictment, US Attorney's Office, Southern District of New York, 16 April 2013, <<https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-charges-34-members-and-associates-two-russian-american-organized>>, accessed 28 August 2019.

If a state does choose to allow online gambling, international standards set by the Financial Action Task Force (FATF) require it to subject casinos, including online casinos, to AML/CTF regulation. The FATF specifies that this should include the following measures, at a minimum:

- ‘Casinos should be licensed.
- Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from [controlling] a casino.
- Competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements’.²³

In accordance with the FATF Recommendations, casinos should conduct customer due diligence (CDD) ‘when their customers engage in financial transactions equal to or above USD/EUR 3,000’.²⁴

In the EU, the 4th Money Laundering Directive (as amended) requires member states to regulate ‘providers of gambling services’, including online gambling. However, it enables them to ‘exempt, in full or in part, providers of certain gambling services from [AML/CTF regulations] on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services’.²⁵

Having availed itself of this option, the UK only extends AML/CTF rules to casinos,²⁶ which are subject to the Gambling Commission’s supervision. In relation to non-casino online gambling, this is paradoxical since the Gambling Commission has recognised these activities as posing high risk. In practice, the effects of this anomaly are attenuated by the Gambling Commission’s requirement that online gambling operators other than casinos must also have AML/CTF controls in place as a precondition for obtaining the licence to operate in Great Britain, as summarised in Table 2.²⁷

23. FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation’, June 2019, Recommendation 28, pp. 21–22.

24. FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation’, June 2019, Interpretive Note to Recommendation 22 (DNFBPS – Customer Due Diligence), p. 84.

25. European Parliament and Council of the European Union, ‘Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorism Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC’, *Official Journal of the European Union* (L 141/73, 5 June 2015), Article 2.

26. As defined in ‘Gambling Act 2005 (UK)’, section 65(2).

27. Gambling Commission, ‘Licence Conditions and Codes of Practice’, October 2018, Licence Condition 12 (Anti-Money Laundering).

Table 2: Gambling Regulation in Great Britain

Gambling Business	Gambling Regulation	AML/CTF Regulation
Casinos	Regulated by the Gambling Commission on the basis of the Gambling Act 2005, including gambling operators that are based overseas but provide facilities that are being used in Great Britain and know that those facilities are being so used.	Subject to Money Laundering Regulations 2017.
Non-Casino Gambling Operators		Not subject to Money Laundering Regulations 2017 but required by the Gambling Commission to comply with AML/CTF rules contained in the Gambling Commission's 'Licence Conditions and Codes of Practice'.

Sources: 'Gambling Act 2005 (UK)', sections 33 and 36; Money Laundering Regulations 2017 (UK); Gambling Commission, 'Licence Conditions and Codes of Practice'.

Territorial Reach of Regulation

When subjecting online gambling operators to AML/CTF regulation, states need to decide whether they wish to cover those businesses that are incorporated beyond their borders and, if so, under what conditions. For instance, online gambling operators whose facilities are being used in Great Britain fall within the Gambling Commission's regulatory ambit and commit an offence if they fail to obtain a licence from the Gambling Commission.

The rationale for this expansive approach is evident. Given the cross-border nature of online gambling, states can adopt such rules to prevent their residents from using money-laundering opportunities that may be offered by overseas businesses. However, two interviewees from two different countries argued in favour of making a distinction between online gambling operators who market their services in a given jurisdiction, in which case they should be subject to its AML/CTF regulation, and those who passively accept customers from that jurisdiction.²⁸ No such distinction exists in Great Britain under the Gambling Act 2005.

In deciding whether a state wishes to extend its AML/CTF regulation to overseas customers, it needs to take account of its practical ability to enforce the rules. One regulator indicated that their agency's enforcement capacity was bolstered by the good working relationships it enjoyed with regulators in major European jurisdictions which host online gambling operators.²⁹ In contrast, another regulator interviewed requires sufficient presence in the jurisdiction as a precondition

28. Author interview with consultant C, London, 4 April 2019; author telephone interview with academic A, 20 May 2019.

29. Author interview with regulator A, European country, 13 February 2019.

for licensing, which ensures that it has practical leverage to address non-compliance.³⁰ It is also important to note that, if a gambling company is licensed by several regulators, each of them will normally assess its AML/CTF compliance on its own, independent of the opinion of the regulator in the country of that company's incorporation.³¹

This difference in approach can be explained by the local context. Whereas the former jurisdiction has a sizeable population of customers who gamble online with foreign operators (and hence is particularly interested in preventing those customers from using online gambling for financial crime), the latter is an online gambling hub oriented towards servicing overseas customers (and is therefore mostly concerned with protecting its reputation as a well-regulated jurisdiction).

30. Author telephone interviews with FIU officer B and regulator B, 7 June 2019.

31. Intervention from a regulator at the RUSI workshop on money laundering through online businesses, London, 10 May 2019.

II. Risks and Mitigation

FOLLOWING AN OVERVIEW of the AML/CTF regulatory regime provided above, this chapter considers in greater detail financial crime risks faced by online gambling operators, as well as measures typically taken to mitigate them. These risks can be divided into operator-related risks and customer-related risks. Since the former facilitates the latter, the dividing line between the two can be blurred, but it provides a convenient categorisation for the purposes of this discussion.

Operator-Related Risks

Criminal Takeover or Collusion

As already mentioned, there is evidence from multiple jurisdictions of criminals running online gaming businesses, ranging from Italian mafia to Israeli cyber-criminals (see Boxes 1 and 2). A distinction should be made between unlicensed online gambling outlets and licensed online gambling outlets controlled by an organised criminal group (OCG).

- **Unlicensed online gambling:** If an unlicensed online gambling business offers services in a jurisdiction that requires it to be licensed, then it operates illegally and the income it generates may be criminal. If that is the case, subsequent use of its income constitutes money laundering. The ease with which the proceeds of illegal gambling can be laundered depends on the ability of financial institutions to identify and investigate those customers whose income may derive from illegal gambling. Other than preventive AML/CTF measures aimed at reducing its profitability, illicit online gambling can only be disrupted through law enforcement action.
- **Licensed online gambling:** The risk of licensed operators being controlled by an OCG or colluding with criminals can only be addressed through regulatory controls, such as fit-and-proper tests, and law enforcement action.

Box 1: Criminal Infiltration of Gambling

Between 2015 and 2018, Italian police carried out spates of arrests in connection with illegal online gambling or money laundering through online gambling. These enforcement actions, which showcase the extent of OCG penetration of online gambling, include: 68 arrests and the seizure of over €1 billion in assets in a number of jurisdictions in November 2018 as a result of at least three mafia families' involvement in running online gambling outlets licensed in Malta; over 60 arrests and €20 million seized in law enforcement action against Malta-registered online gambling businesses allegedly owned by 'Ndrangheta affiliates in May 2017; and analogous charges against 41 people arrested and the seizure of €2 billion in November 2015.

On the other side of the Atlantic, the US Department of State alleges that sports gambling companies in Costa Rica are 'suspected of laundering millions of dollars'. In 2016, the Department of State also reported that 'Curaçao's gambling industry is allegedly intertwined with the mafia'. The same year, Curaçao's then-prime minister was found guilty of accepting bribes from a casino owner and related money laundering, with the verdict upheld by the Supreme Court in 2018.

Sources: Ted Menmuir, 'AgiproNews Italian View: Gambling Left Red-Faced by Mafia Investigations', SBC News, 28 November 2018; Nathan Joyes, 'Italy Arrests 68 Online Gambling Mafia Members', Gambling Insider, 14 November 2018; Matteo Civillini, 'Italy Seizes Millions from Online Gambling Business', Organized Crime and Corruption Reporting Project (OCCRP), 18 May 2018; Matteo Civillini et al., 'Gambling on Crime', OCCRP, 24 July 2019; Europol, From Suspicion to Action: Converting Financial Intelligence into Greater Operational Impact (Luxembourg: Publications Office of the European Union, 2017), p. 14; US Department of State, 'International Narcotics Control Strategy Report: Volume II, Money Laundering', March 2019, pp. 82, 87; US Department of State, 'International Narcotics Control Strategy Report: Volume II, Money Laundering', March 2016, p. 105.

Box 2: Gery Shalon's Online Casinos

According to a US indictment, an Israeli cyber-criminal group that carried out several large-scale cyber attacks, including the hacking of JP Morgan in 2014, also operated 12 illicit internet casinos. The group's casino business alone allegedly generated hundreds of millions of dollars in criminal income. The group's alleged mastermind, Gery Shalon, is in US custody awaiting trial as of March 2019.

Sources: US vs. Gery Shalon et al., 'Sealed Superseding Indictment', New York Southern District Court, SI 15 Cr. 333 (LTS), 22 October 2015, paras. 17–18; Helena Bedwell, Christian Berthelsen and Michael Riley, 'JPMorgan Hack Suspect Is Helping the US. Here's What He May Offer', Bloomberg, 16 March 2019; Mathew J Schwartz, 'Accused JPMorgan Chase Hacker Plans to Plead Guilty', Bank Info Security, 20 September 2019.

Several highly publicised instances of OCG infiltration of online gambling bring into stark relief the challenges of applying rigorous fit-and-proper controls faced by gambling authorities. One academic interviewed for this research has argued that, although countries are supposed to

carry out fit-and-proper tests for gambling operators, in reality they are less stringent than those applied to, for instance, financial institutions.³² A slightly different view was expressed by a law enforcement officer who suggested that most regulators, not only those of gambling, occasionally find it difficult to identify involvement of individuals who are not themselves OCG members but have hidden criminal connections.³³

These challenges can be particularly acute in online gambling hubs, where the prominence of online gambling may not always be matched by the resources available to ensure the market's integrity. In some instances, online gambling operators are incorporated in special economic zones where AML/CTF controls are in practice more relaxed compared to the rest of the country, such as the First Cagayan Special Economic Zone in the Philippines.³⁴

Criminal infiltration of regulated businesses, which has already been the subject of some academic research,³⁵ is a separate issue that goes beyond the scope of this paper. But since regulators of various sectors face the similar challenge of ensuring that their licensing and fit-and-proper controls are robust, it may be helpful for them to explore if they can further advance the sharing of best practices in relation to fit-and-proper checks and background investigations.

Business-to-Business Vulnerabilities

A 2019 *Financial Times* investigation reveals how its reporters could win money through a regulated UK sports betting company without disclosing their identity. The arrangement involved three betting companies:

- Company A, a UK-regulated betting company forming part of a FTSE 100-listed group.
- Company B, its business-to-business (B2B) partner, which mirrors the bets available on Company A's website under an agreement with Company A.
- Company C, a Curaçao-regulated betting company that accepted the payment from the reporters and provided them with login details for placing the bet with Company B (and, hence, indirectly with Company A).³⁶

32. Author telephone interview with academic A, 20 May 2019.

33. Author interview with non-UK law enforcement officer B London, 29 August 2019.

34. Fred Lord, "Free for All Zone" – Free Trade & Special Economic Zones (FTZ & SEZ) International Online Betting Operators & Gambling', 5th OECD Task Force for Countering Illicit Trade, 27 March 2017, p. 8.

35. Ernesto U Savona and Michele Riccardi (eds), 'Mapping the Risk of Serious and Organised Crime Infiltration in European Businesses – Final Report of the MORE Project', Transcrime and Università Cattolica del Sacro Cuore, 2018, p. 53. Note that both land-based and online gambling are among vulnerable sectors.

36. Antonia Cundy and Paul Murphy, 'Backdoor to Betfair: How to Win £2,000 with no Compliance Checks', *Financial Times*, 2 July 2019.

In essence, the reporters were able to exploit company C's wilful non-compliance with AML/CTF obligations and Company B's deficient AML/CTF controls to place bets with UK-regulated company A. This casts doubt on the robustness of due diligence that company A does on its B2B partners. Against this background, it is worth noting that one of the regulators interviewed for this research specifically highlighted its efforts to undertake fit-and-proper checks on B2B partners of the operators it licensed.³⁷

The ability to place anonymous bets can be attractive for criminals who wish to gamble for fun or customers from countries where gambling is illegal. Whether this arrangement is also appealing to those who aim to disguise the criminal provenance of their funds is likely to depend on: whether the customer is able to either place and withdraw funds without making a bet or minimise the risks of losing money through bets; which of the companies (A, B or C) is making the payout to the customer; and how likely that transfer is to raise concerns with the customer's financial institution.

Customer-Related Risks

Lifestyle Gambling with Criminal Proceeds

Two interviewees argued that, in the absence of criminal infiltration or collusion, the main money-laundering risk faced by online gambling businesses was customers using criminal proceeds to gamble for fun.³⁸ This suggestion is indirectly borne out by published research, which indicates that opportunities for more systematic and large-scale money laundering through online gambling are limited.

For instance, Michael Levi's study in 2009 concluded that money-laundering opportunities in online gambling were 'modest', 'partly a result of the greater recording of transactions in this industry than in most others, and partly the consequence of legitimate firms being subject to regulation'.³⁹ A Moneyval report published four years later has reaffirmed that view.⁴⁰ These findings are concordant with a 2013 study of land-based casinos in Australia, which similarly found that their financial crime risks overwhelmingly concerned lifestyle gambling rather than systematic, large-scale money laundering.⁴¹

37. Author telephone interview with FIU officer B and regulator B, 7 June 2019.

38. Author interview with consultant C, London, 4 April 2019; author telephone interview with academic A, 20 May 2019.

39. Michael Levi, 'Money Laundering Risks and E-Gaming: A European Overview and Assessment', Cardiff University, September 2009, p. 6.

40. Moneyval, 'The Use of Online Gambling', p. 15.

41. Christopher Murphy, *Money Laundering and the Casino Industry: Findings from a Doctoral Study* (Freiburg im Breisgau: Max Planck Institute for Foreign and International Criminal Law, 2013), pp. 14–17.

Lifestyle gambling can be intertwined with problem gambling as a person suffering from gambling addiction may feel drawn to crime to continue gambling. CDD measures, such as knowing the customer and (if necessary) their source of funds, are therefore indispensable for the prevention of both money laundering and problem gambling. By way of example, the link between AML/CTF measures and prevention of problem gambling came to the fore in the Gambling Commission's enforcement action against Ladbrokes (see Box 3).

Box 3: Ladbrokes Enforcement Action

On 31 July 2019, the Gambling Commission published the findings of its investigations into Ladbrokes Coral Group's handling of seven customers' accounts between November 2014 and October 2017. The Gambling Commission identified, among others, the following instance: 'Despite one customer spending £1.5m over [two years and 10 months], Coral did not ask the customer to evidence their source of funds and could not provide evidence of any social responsibility interactions being carried out'.

This and other failings led to the payment of £4.8 million in lieu of a financial penalty and divestment of £1.1 million in profits as a result of breaches of both AML/CTF obligations and the Social Responsibility Code. By the time the Gambling Commission commenced its investigation, the ownership of Ladbrokes Coral Group had changed hands and there was no allegation of impropriety on the part of its current owner, GVC.

Source: Gambling Commission, 'Ladbrokes Coral Group to pay £5.9m for Past Failings in Anti-Money Laundering and Social Responsibility', 31 July 2019, <<https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/ladbrokes-coral-group-to-pay-59m>>, accessed 28 August 2019.

To address these twin risks, online gambling operators typically resort to enhanced due diligence (EDD) measures once a certain threshold is reached. In the UK, this threshold differs across businesses, with the result that while one company opts for £5,000, another chooses £50,000.⁴² The difficulty of only relying on thresholds is that the customer's activity may be spread across a number of operators, each of whom will only see a partial picture of that customer's activity; nor does reliance solely on a monetary threshold allow due regard to other factors making up a customer's risk profile.⁴³

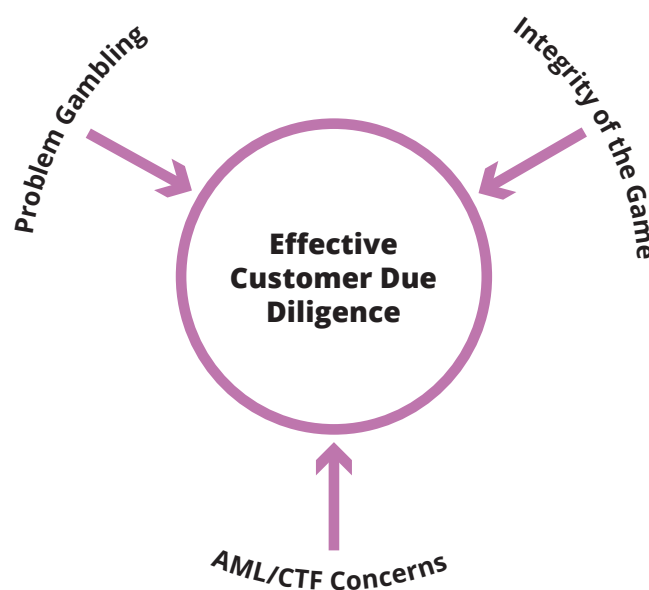
In the UK, the absence of strict regulatory prescription in relation to EDD thresholds is a consequence of the Gambling Commission being a principles-based regulator that encourages the application of a risk-based approach. However, there are concerns among some gambling businesses that, in practice, the risk-based approach tends to morph into subjectivity and

42. Intervention from a casino representative at RUSI workshop on money laundering through online businesses, London, 10 May 2019.

43. GAMLG, 'GAMLG's AML Risk Assessment', p. 12.

unjustified inconsistency.⁴⁴ Once EDD is triggered, additional checks are undertaken to verify whether the customer can afford their gambling, for instance by comparing the amounts with average salaries in the relevant postcode area or the customer's professional activity.⁴⁵

Figure 1: Gambling Businesses' Incentives to Conduct Effective CDD



Source: Author's research.

The Remote Gambling Association has developed guidance on best practice in using behavioural analysis to identify problem gambling. The techniques recommended in the guidance rely, among other things, on detecting atypical gambling patterns, for example in relation to amounts, timing or frequency of gambling.⁴⁶ An analogous approach is useful for AML/CTF purposes, although specific risk indicators may be different.

Use of Stolen Cards

The use of stolen credit or debit card details is a risk that, while common to online businesses and not gambling-specific, has manifested itself in the gambling context. In a case from the

44. Intervention from a gambling business and money-service business representatives at RUSI workshop on money laundering through online businesses, London, 10 May 2019.

45. Author interview with consultant C, London, 4 April 2019.

46. Remote Gambling Association, 'Behavioural Analytics: RGA Good Practice Guidelines', October 2018, pp. 4–5.

early 2000s, three convicted British terrorist sympathisers, Tariq Al-Daour, Waseem Mughal and Younes Tsouli, had earned up to £2 million by stealing credit card details and reportedly used them for online gambling by the time of their arrest in 2005.⁴⁷ But, according to Levi, many of their attempts to launder money through online gambling websites were in fact unsuccessful and led to suspicious activity reports (SARs) being filed.⁴⁸

More recently, during the interviews for this research, a European FIU suggested that the use of stolen cards was the most widespread financial crime issue faced by online gambling operators. As a result, the largest proportion of SARs submitted by online gambling operators in that jurisdiction pertains to fraud.⁴⁹ These reports tend to concern activity of users located in several Eastern European and Latin American countries.⁵⁰

Furthermore, that country's gambling authority has detected the use of multiple debit/credit cards linked to place funds in a single gambling account. At least some of those card details are likely to be fraudulently obtained. In resorting to this technique, criminals exploit the fact that some online gambling operators have (or claim to have) no ability to check the name to which the card was issued and match it to the account holder's name.⁵¹ Importantly, it is unknown whether criminals seeking to use stolen cards are more likely to target online gambling than other internet businesses; nor is it known whether they prefer businesses incorporated or regulated in certain jurisdictions.⁵²

The experiences of gambling operators (and, indeed, other online businesses) in connection with identifying stolen card details vary. In the course of the research carried out for this paper, a contrast became apparent between online gambling operators and cryptocurrency businesses, with the latter being more likely to use automatic scouring of the Dark Web to proactively identify stolen card details.⁵³ That said, the regulator in a European jurisdiction reported seeing instances of online gambling companies doing exactly that.⁵⁴ It is of interest that, at the time of writing the Gambling Commission is consulting on its intention to ban the use of credit cards

47. MHA Consulting, 'The Threat of Money Laundering and Terrorist Financing Through the Online Gambling Industry', June 2009, p. 31.

48. Levi, 'Money Laundering Risks and E-Gaming', p. 10.

49. Author interview with FIU officer A, European country, 16 May 2019. Fraud was also the most widespread category of predicate offences in another jurisdiction as per FIU officer D, written reply, 12 August 2019. However, it is unclear whether those suspicions referred specifically to the use of stolen bank cards.

50. Author interview with FIU officer A, European country, 16 May 2019.

51. Author telephone interview with regulator C, 17 June 2019.

52. Author interview with FIU officer A, European country, 16 May 2019.

53. In relation to gambling: author interview with consultant C, London, 4 April 2019. In relation to cryptocurrency businesses: author telephone interview with cryptocurrency compliance officer A, 4 April 2019; intervention from a representative of a blockchain analysis company at RUSI workshop on money laundering through online businesses, London, 10 May 2019.

54. Author telephone interview with regulator C, 17 June 2019.

for gambling, but the issue is entirely that of preventing irresponsible gambling and borrowing, with no effect anticipated on the use of debit cards.⁵⁵

In either case, if a gambling business obtains information on compromised bank cards, it should be able to use it and ensure that stolen card details are blocked. Representatives of two payment processing companies interviewed for this research, including a cryptocurrency company, suggested that proactively identifying stolen card details can be redundant because many of them are never used; hence those companies' preference for technology that aims to block fraudulent card transfers in real time.⁵⁶

Peer-to-Peer Value Transfers

While some gambling products only allow customers to play against the house, others, such as online poker, provide opportunities for peer-to-peer value transfer through deliberate 'losses'. In its consecutive risk assessments, the Gambling Commission assessed risks associated with such peer-to-peer transfers as high.⁵⁷ Two interviews with industry insiders suggest that casinos deem themselves effective in mitigating these risks through use of algorithms that detect player collusion, which is a key measure aimed at preserving the integrity of the game.⁵⁸ But another AML/CTF expert, who worked for an online gambling company in the past, expressed misgivings about this assessment. In that expert's opinion, gambling operators had no way of understanding how effective they were in preventing poker collusion, beyond the obvious fact that 'they detect 100% of the cases they detect'.⁵⁹ The optimistic view of the industry's defences was also queried by one European regulator, who argued that peer-to-peer transfers of small amounts, while unsuitable for large-scale money laundering, can nonetheless pose a terrorist-financing risk. That regulator is therefore considering a thematic review of peer-to-peer games.⁶⁰ This is thus an area where the risk perceptions among regulators and industry players appear to diverge.

55. Gambling Commission, 'Gambling Online with Credit Cards', 24 July 2019, <<https://www.gamblingcommission.gov.uk/news-action-and-statistics/News/gambling-online-with-credit-cards>>, accessed 28 August 2019.

56. Author interview with payment processing company A, London, 2 July 2019; author interview with cryptocurrency compliance officer B (with prior experience of the gambling sector), London, 5 September 2019.

57. Gambling Commission, 'Money Laundering and Terrorist Financing Risk Within the British Gambling Industry', pp. 33, 43.

58. Author interview with consultant C, London, 4 April 2019; author telephone interview with academic A, 20 May 2019. The view is also reflected in the GAMLG's assessment of the residual risk posed by such activity as 'low', assuming effective AML/CTF controls are in place, see GAMLG, 'GAMLG's AML Risk Assessment', p. 13.

59. Author interview with cryptocurrency compliance officer B (with prior experience of the gambling sector), London, 5 September 2019.

60. Author telephone interviews with FIU officer B and regulator B, 7 June 2019.

Use of False IDs

The use of false IDs is a common risk that online gambling operators face from customers who wish to hide their identity. Its mitigation can be challenging for those online gambling operators that service customers from a wide range of countries.⁶¹ Conversely, a UK-based online casino whose customers are overwhelmingly British citizens did not see false IDs as a significant challenge.⁶²

Overall across the sector, the UK-based Gambling Anti-Money Laundering Group assesses the risk of ‘unverified or front accounts’ as high in terms of inherent risk but low if proper mitigation controls are applied.⁶³ These controls typically rely on the services of third-party providers that enable ID verification. As a result, they are only as good as the respective third-party provider, who is unlikely to have equally effective coverage of all countries’ IDs.⁶⁴ This is a challenge that is common to various internet businesses, including financial technology (FinTech) companies, which have started complementing traditional ID verification (such as database cross-checking) used with biometrics and voice recognition. While these measures are superfluous for businesses with limited false ID risks (for instance, by virtue of the jurisdictions from where they draw their customers), other online gambling operators may wish to consider novel, FinTech-type techniques.

Use of Cryptocurrency

Potential adoption of cryptocurrency payments in online gambling is occasionally viewed as a financial crime risk.⁶⁵ This is largely due to the perception that cryptocurrency offers a degree of anonymity, which is only true to some extent and depends on the cryptocurrency in question.⁶⁶ Regardless of what payment means a customer uses, a gambling company can still identify who the customer is, ask where the money comes from (including by requesting necessary supporting documents), and report suspicious activities to law enforcement.

61. Gambling Commission, ‘Money Laundering and Terrorist Financing Risk Within the British Gambling Industry’, pp. 31, 48.

62. Intervention from a casino representative at RUSI workshop on money laundering through online businesses, London, 10 May 2019.

63. GAMLG, ‘GAMLG’s AML Risk Assessment’, p. 11.

64. Intervention from a large money-service business representative at RUSI workshop on money laundering through online businesses, London, 10 May 2019.

65. See, for example, Peter M German, ‘Dirty Money: An Independent Review of Money Laundering in Lower Mainland Casinos Conducted for the Attorney General of British Columbia’, Government of British Columbia, March 2018, pp. 178–79 (the report notes the risks of cryptocurrency even though it is concerned with land-based casinos).

66. For details, see Anton Moiseienko and Kayla Izenman, ‘From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency’, *RUSI Occasional Papers* (September 2019).

In this context, it is necessary to distinguish between licensed and unlicensed gambling operators. Among licensed operators, the adoption of cryptocurrency as a payment means remains limited to date, although one interviewee suggested that an increasing number of online casinos, including those based in the gambling hubs of Curaçao and Malta, sought to enable cryptocurrency payments.⁶⁷ Some regulators – for instance, in the Isle of Man – have expressly allowed the use of cryptocurrency in online gambling.⁶⁸ This comes with certain restrictions:

- An Isle of Man-regulated gambling business should not provide exchange services; it should only make payouts in the same currency in which it accepted the customer's payment. However, since some cryptocurrency users generate a new address for every transaction to protect their privacy, it may not always be easy for a gambling business to identify whether the payout is being made to an address controlled by the gambler or a third party.⁶⁹
- It should only use regulated cryptocurrency exchanges to minimise the possibility that it will unwittingly accept funds that stem from criminal misconduct.⁷⁰

If online gambling providers did enable cryptocurrency exchange, that would not be without precedent. Land-based casinos frequently provide financial services such as currency exchange.⁷¹ Similarly to financial services provided by land-based casinos, online gambling operators' financial/cryptocurrency activities should be supervised by an agency with sufficient wherewithal and expertise, which could create challenges for gambling supervisors. Furthermore, licensed operators would need to ensure they incorporate cryptocurrency-specific information, such as wallet addresses, in their SAR filings for them to be as informative as possible.⁷²

Meanwhile, unlicensed operators can either generate criminal proceeds (of illegal gambling) themselves or serve as receptacles of other criminal proceeds. For instance, research published in 2018 suggests that, out of 163 key Bitcoin addresses used to deposit the proceeds of the top 15 Ransomware families, 47 addresses were gambling websites.⁷³ These websites tend to focus

67. Author interview with cryptocurrency compliance officer B (with prior experience of the gambling sector), London, 5 September 2019.

68. Isle of Man Gambling Supervision Commission, 'AML/CFT Guidance for Virtual Currencies', May 2017, pp. 5–7.

69. Author interview with cryptocurrency compliance officer B (with prior experience of the gambling sector), London, 5 September 2019.

70. Isle of Man Gambling Supervision Commission, 'AML/CFT Guidance for Virtual Currencies', p. 5.

71. FATF and Asia/Pacific Group, 'Vulnerabilities of Casinos and Gaming Sector', p. 41.

72. See Kenneth A Blanco, 'Prepared Remarks of FinCEN Director Kenneth A. Blanco', speech given at the 12th Annual Las Vegas Anti-Money Laundering Conference, 13 August 2019, <<https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-12th-annual-las-vegas-anti>>, accessed 28 August 2019.

73. Masarah Paquet-Clouston, Bernhard Haslhofer and Benoit Dupont, 'Ransomware Payments in the Bitcoin Ecosystem', paper presented to the 17th Annual Workshop on the Economics of Information Security (WEIS), Innsbruck, Austria, 18–19 June 2018, p. 6.

on Bitcoin transactions, collect no identifying information on their customers and frequently do not disclose their own location, which enables them to fulfil functions similar to those of Bitcoin mixers.⁷⁴ In short, the risks posed by these unlicensed operators are entirely distinct from the risks of licensed businesses adopting cryptocurrency as a means of payment, which can be adequately addressed through regulation, as described above.

74. CipherTrace, 'Q2 2018 Cryptocurrency Anti-Money Laundering Report', 2018, <<https://ciphertrace.com/q2-2018-cryptocurrency-anti-money-laundering-report/>>, accessed 28 August 2019.

III. Interaction with Financial Institutions

DUE TO THE non-face-to-face nature of online gambling, customers invariably rely on financial institutions, such as banks or money service businesses, to make or receive payments. This is in contrast to land-based gambling, which can be cash-intensive,⁷⁵ and gives financial institutions a key role in precluding access to unlicensed gambling operators, which is discussed in this chapter, with several references to the US experience of enforcing online gambling prohibitions.

The Importance of Payment Processing

In the *Financial Times* investigation cited previously, the payment to Company C was made through the e-payment service Neteller, one of the leading payment processors for online gambling.⁷⁶ In the case at hand, Company C was a Curaçao-regulated business and no suggestion of impropriety on Neteller's part is implied in either this paper or the *Financial Times* article. But Neteller's history offers a useful insight into the role of payment processors in preventing access to unlicensed gambling operators.

In January 2007, Neteller's two founders were indicted and subsequently convicted in the US on charges of money laundering related to illegal gambling due to the company's role in processing gambling-related payments,⁷⁷ while it forfeited \$136 million and admitted wrongdoing in an out-of-court settlement.⁷⁸ The US action against Neteller was predated by the enactment of the Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA), which made it a crime for a 'person engaged in the business of betting or wagering' to 'knowingly accept' funds in connection with 'unlawful Internet gambling'.⁷⁹

75. It is possible for customers to gamble online using cash if an online gambling operator collaborates with a land-based one. This, however, can be seen as a risk stemming from the involvement of a land-based casino. See Simon Planzer, 'Anti-Money Laundering and Online Gambling: Guidance on How to Implement Broad and Indistinct AML Notions in Regulatory Practice', 1 October 2017, <<https://ssrn.com/abstract=3048303>>, accessed 28 August 2019.

76. Cundy and Murphy, 'Backdoor to Betfair'.

77. United States Attorney for the Southern District of New York, 'U.S. Charges Two Founders of Payment Services Company with Laundering Billions of Dollars of Internet Gambling Proceeds', 16 January 2007.

78. Bob Pajich, 'Full Statements from NETELLER and USAO Here', *Card Player*, 18 July 2007, <<https://www.cardplayer.com/poker-news/2464-full-statements-from-neteller-and-usao-here>>, accessed 28 August 2019.

79. 'Unlawful Internet Gambling Enforcement Act 2006 (US)'.

Transaction Laundering

In 2011, on a day commonly referred to as the ‘Black Friday’ of online poker, the US Department of Justice (DOJ) brought criminal and civil charges on the basis of the UIGEA against three major online poker businesses. It also indicted individuals who were running payment-processing companies that enabled those poker companies to make payments through US banks. To achieve that, those ‘highly compensated’ payment processors allegedly engaged in transaction laundering, that is, concealing the real nature of one’s business to obtain access to payment facilities. Specifically, they ‘lied to banks about the nature of the financial transactions they were processing, and covered up those lies, by, among other things, creating phony corporations and websites’.⁸⁰ The DOJ made similar allegations in the Shalon et al. case referenced in Box 2, where the defendants allegedly shunned neither lies nor the corruption of bank officials.⁸¹

Effects of Uncertainty

Financial institutions in the US have the luxury of relative certainty in that only a few states in the US allow online gambling, with a debate ongoing at the time of writing as to the precise limits that the Interstate Wire Act places on online gambling in the US.⁸² In those jurisdictions where online gambling is legal and more widespread than in the US, it may be challenging for financial institutions to distinguish between transactions involving licensed gambling operators and those involving unlicensed ones.

Depending on the country’s gambling regime, financial institutions may need to be able to stop their customers from transacting with unlicensed online gambling operators. Given their understanding of the online gambling landscape, regulators play a vital part in supporting these efforts. For instance, one regulator shares information on non-compliant online gambling operators with financial institutions (via a public–private partnership) and internet service providers to prevent users from either making payments to those operators or accessing their services in the first place.⁸³

The treatment of illegal online gambling transactions among financial institutions in a single country does not always appear consistent. For instance, in Germany and Russia there are online forums and YouTube videos that point gamblers to banks or payment processors that are

80. US Attorney’s Office, ‘Manhattan U.S. Attorney Charges Principals of Three Largest Internet Poker Companies with Bank Fraud, Illegal Gambling Offenses, and Laundering Billions in Illegal Gambling Proceeds’, 15 April 2011. The defendants accused of running payment processing companies later pleaded guilty to various charges. See Steven Stadbrooke, ‘Black Friday Defendant Chad Elie Pleads Guilty to Conspiracy’, CalvinAyre.com, 27 March 2012.

81. US vs. Gery Shalon et al., ‘Sealed Superseding Indictment’, para. 30.

82. ‘Interstate Wire Act 1961 (US)’; State of New Jersey, Office of the Attorney General, ‘AG Grewal Letter to Trump Administration: New Opinion Regarding Online Gambling is “Wrong” and “Deeply Troubling”’, 5 February 2019.

83. Author interview with regulator A, European country, 13 February 2019.

amenable to being used for illicit gambling transactions.⁸⁴ Likewise, an academic interviewed for this research has asserted that some financial institutions turn a blind eye to such transfers in return for fees.⁸⁵

This underscores the need for regulators to both strengthen gambling operators' compliance efforts through information sharing and create a credible deterrent against flouting regulatory obligations. For that credible deterrent to be in place, regulators need to first identify gambling businesses subject to their regulation, both within the respective country and, if necessary, outside it. One regulator has indicated that it operates an intelligence unit, which cooperates with LEAs, to that end.⁸⁶ Another regulator receives notifications from trust and company service providers about the incorporation of gambling companies and has on occasion made use of its right to object to incorporation.⁸⁷

84. See Gamblejoe, 'Ein- und Auszahlungsmethoden: Bank kündigt konto', <<https://www.gamblejoe.com/forum/online-casinos/einzahlung-auszahlung/bank-kundigt-konto-76334/2/>>, accessed 15 October 2019 (German internet users giving advice to an online gambler whose bank account was closed down); ПОКЕРНЫЙ МАГ [*Pokernyi Mag; Poker Wizard*], 'ВЫВОД ДЕНЕГ НА Skrill кошелек/ АЗАРТНЫЕ ИГРЫ/ ОБЗОР КАК ПОЛУЧИТЬ СРЕДСТВА' [Cashing out into Skrill Wallet/Gambling/ Review of Cashing Out Techniques], YouTube, <<https://www.youtube.com/watch?v=6gnYlwjF98U>>, accessed 15 October 2019 (a Russian poker player sharing advice on playing online).

85. Author telephone interview with academic A, 20 May 2019.

86. Author interview with regulator A, European country, 13 February 2019.

87. Author telephone interviews with FIU officer B and regulator B, 7 June 2019.

IV. Interaction with Law Enforcement

AS REGULATED BUSINESSES, online gambling operators fulfil a dual function in the AML/CTF regime. Not only are their AML/CTF controls supposed to prevent criminals from using their services to launder criminal proceeds, but if a criminal were to make use of a gambling operator, the latter is supposed to provide intelligence to LEAs through the medium of SARs. Europol refers to gambling businesses among the three non-financial sectors that contribute the greatest rates of SARs.⁸⁸

As they amass SARs, FIUs and LEAs can develop an understanding of financial crime threats that draws on the collective experience across the sector and thus potentially surpasses that of individual gambling businesses. In 2019, an analysis of 250 SARs related to land-based casinos in the area covered by London's Metropolitan Police Service, which focused specifically on the use of gambling by repeat offenders, revealed common reasons for the submission of SARs by gambling operators and financial institutions.⁸⁹ Similar analysis would be helpful in the context of online gambling, particularly in jurisdictions that serve as online gambling hubs. Sharing its insights with regulators and online gambling operators would ensure that SARs contribute not only to LEAs' work but also to the industry's understanding of the threat landscape. The importance of SAR analysis, particularly in online gambling hubs, has been highlighted in Moneyval's 2019 mutual evaluation review of Malta, which noted in its 'key findings':

There are also some concerns regarding the use of suspicious transaction reports (STRs), mainly from the remote gambling sector concerning non-residents, as these cases are not sufficiently considered to identify possible ML [money laundering] taking place through Malta.⁹⁰

The number of SARs received in major European online gambling jurisdictions (see Table 3), which is in the hundreds (except in the UK), suggest that such analysis can be feasible with a relatively modest commitment of resources.

88. Europol, 'From Suspicion to Action: Converting Financial Intelligence into Greater Operational Impact', 2017, p. 14.

89. Graham Edwards, 'Suspicious Activity Reports (SARs) Analysis on the Criminal Use of the Gaming (Casino) Sector', *ACAMS Journal* (Vol. 1, No. 1, 2019).

90. Moneyval, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Malta – Fifth Round Mutual Evaluation Report', July 2019, p. 6.

Table 3: SAR Submission Rates from Gambling Operators

Year	Jurisdiction	Number	Details
2018	UK	3,768 (less than 1% of all SARs)	The figure covers both online and land-based gambling. Only casinos are subject to AML/CTF regulation, but both regulated and non-regulated gambling businesses have filed SARs.
2018	Isle of Man	248 (18% of all SARs)	The figure covers online gambling specifically. Land-based gambling companies filed three SARs.
2017	Gibraltar	779 (47% of all STRs)	The figure covers both online and land-based gambling. All of these STRs relate to money laundering rather than terrorist financing.
2016	Malta	Approximately 100 (18% of all STRs)	No exact figures provided in the National Risk Assessment. This covers both online and land-based gambling.

Sources: Isle of Man Financial Intelligence Unit, 'Annual Report 2017/2018', 2018, p. 15; HM Government of Gibraltar, '2018 National Risk Assessment: Money Laundering and Terrorist Financing Risks', 14 September 2018, p. 8; National Crime Agency, 'Suspicious Activity Reports (SARs) Annual Report 2018', 2018, p. 6; Republic of Malta, 'Results of the ML/TF National Risk Assessment', p. 24.

Conclusions and Recommendations

LIKE OTHER BUSINESS sectors, online gambling faces some risk of criminal exploitation. At its simplest, criminal abuse of this sector involves the use of criminal proceeds for gambling, similar to how any other services may be purchased using criminal income. It is inevitable that small transactions involving criminal proceeds can go under the radar of both gambling operators and financial institutions that process payments.

In the case of larger transactions or atypical behaviour, however, gambling operators' CDD processes can make a meaningful contribution to the detection of either financial crime or other undesirable behaviour, such as problem gambling. For that, consistently high standards are necessary across the industry, including in relation to monetary thresholds for EDD and the gambling operators' ability to identify false IDs. Given the vital importance of ensuring this consistency and thus preventing the displacement of crime towards operators with less stringent controls, it is a prime candidate for gambling regulators' attention.

Among other challenges, the use of stolen cards presents an apparently ubiquitous threat, with online gambling operators currently taking varying approaches to its detection. The robustness of their controls is essential to ensuring they do not become the avenue of choice for cyber-criminals to monetise stolen card details. Furthermore, given that other online businesses are likely to face the same problem, in conducting this analysis regulators could both learn from other sectors' experience and publish findings that would be of interest to other online businesses, not only online gambling operators.

Recommendation 1: In order to facilitate consistently high AML/CTF standards across the industry, gambling regulators should undertake thematic reviews of:

- **Online gambling operators' CDD practices.**
- **Online gambling operators' ability to detect the use of stolen card details.**

Publication of such reviews, as well as their dissemination via international groups such as the International Association of Gaming Regulators and the Gaming Regulators European Forum, can also contribute to increased cohesion of AML/CTF controls across major gambling jurisdictions, which will mitigate possible displacement effects.

While this paper identifies these two issues as particularly deserving of further study, it is possible that other matters will arise as the industry's risk landscape becomes better understood. FIUs and/or law enforcement agencies can contribute to the collective understanding of financial crime risks through the analysis of online gambling-related SARs, whether submitted by gambling

operators or other regulated sectors. For all the imperfections of a database that is based on reporters' subjective suspicions, SARs offer a rare source of data on the suspicious activity that businesses in the sector have to contend with.

Recommendation 2: FIUs and/or law enforcement agencies should analyse SARs related to online gambling to identify trends in suspicious activities. This analysis should then be shared with the regulators and inform their engagement with the sector, for instance areas for thematic review, as well as be disseminated to online gambling operators.

While maintaining high AML/CTF standards in regulated gambling businesses is indispensable, regulators also need to consider opportunities for limiting customers' access to those gambling businesses that fall short of regulatory requirements. Given their role in payment processing, financial institutions represent a natural choke point. In countries where gambling is legal but regulated, they can – and, one may argue, should – play a part in preventing consumers from gambling with unregulated service providers, owing to both financial crime and problem gambling concerns.

Recommendation 3: Gambling regulators that do not yet do so should consider arrangements for informing financial institutions about unlicensed gambling operators that illegally offer services in the respective jurisdiction.

Yet even if a financial institution can tell licensed gambling operators from unlicensed ones, it may unwittingly process transactions for a rogue gambling business that claims to carry out some other, non-regulated activity, as was the case in the US 'Black Friday' poker cases. Like many other financial crime risks, this one is by no means unique to gambling and is often referred to as 'transaction laundering', a practice whose effective prevention is vital to ensuring that financial institutions are not unwittingly processing payments for customers of whom they would otherwise steer clear.

Recommendation 4: Financial services regulators should review financial institutions' ability to detect transaction laundering.

The upward trajectory of cryptocurrency may prompt businesses and regulators to consider financial crime implications of employing this payment means for online gambling purposes. If online gambling operators start accepting cryptocurrency, regulators will either need to restrict the range of cryptocurrency-related activities that such businesses are allowed to undertake (for instance, by stipulating that they cannot provide exchange services themselves) or ensure that those activities are adequately supervised, either by the gambling regulator or by another competent authority.

Recommendation 5: Governments should clarify which cryptocurrency activities online gambling operators can undertake and ensure their AML/CTF supervision by a regulator with adequate resources and expertise.

Although all these recommendations are directed at governments (especially regulators) as they shape the private sector's AML/CTF obligations and support its compliance efforts, in the final analysis governments can never substitute for conscientious action by businesses themselves. With all the support they can get from regulators and law enforcement, gambling operators should continue to seek out better knowledge about the financial crime risks they face, regularly take stock of the strength of their responses, and aid law enforcement within the bounds of the law.

About the Author

Anton Moiseienko is a Research Fellow at RUSI's Centre for Financial Crime and Security Studies.