Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Understanding Financial Crime Risks in E-Commerce

Anton Moiseienko

Understanding Financial Crime Risks in E-Commerce

Anton Moiseienko

RUSI Occasional Paper, January 2020

Royal United Services Institute
for Defence and Security Studies

189 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 189 years.

Published in 2020 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, January 2020. ISSN 2397-0286 (Online).

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

This paper forms part of the Financial Crime 2.0 research programme funded by EY and Refinitiv. The author wishes to thank Malcolm Chalmers, Tom Keatinge, Rebecca Marriott and Carsten Ullrich for their helpful comments on an earlier version of the paper. Thanks are also due to those who have generously offered their time to be interviewed for this research, as well as the publications team at RUSI for their excellent editing.

Executive Summary

E-COMMERCE, OR THE sale of goods and services online, has reportedly reached $29 trillion in 2017.[1] In the UK alone, the volume of e-commerce sales in 2017 was estimated at $586 billion.[2] Inevitably, this vast amount of legitimate activity offers opportunities for the concealment of criminal transactions. E-commerce businesses can be exploited for criminal purposes in four major ways:

- Committing fraud against the customer by failing to deliver goods or services.
- Buying goods or services using stolen bank card data.
- Creating e-commerce businesses as a front for illicit transactions (for example, to accept bank card payments for drugs).
- Abusing online marketplaces to move criminally obtained funds (for example, through the sale of computer-generated books sold via Amazon).[3]

Of these criminal modi operandi, the latter two present particular money-laundering and terrorist-financing (financial crime) threats because they involve consensual transactions that are intended to remain undetected. Despite their role in concealing criminal income, these phenomena remain poorly understood.

For instance, there are multiple examples of criminal groups using e-commerce businesses to receive payments for illicit transactions – a criminal typology known as 'transaction laundering' – including the case detected by one of the interviewees of an art-trading company selling illicit drugs online.[4] But, save for a range of enforcement actions by the US Federal Trade Commission (FTC) against complicit payment processors, there is little evidence of a law enforcement or government focus on this issue.[5] As a result, there are no verifiable estimates of how prevalent the problem is, nor is it clear what compliant financial institutions should do to better detect this type of criminal abuse. This stands in contrast to other sectors

1. United Nations Conference on Trade and Development (UNCTAD), 'Global E-Commerce Sales Surged to $29 Trillion', 29 March 2019, <https://unctad.org/en/pages/PressRelease.aspx?OriginalVersionID=505>, accessed 23 October 2019.
2. S O'Dea, 'E-Commerce in the United Kingdom (UK) – Statistics & Facts', 31 July 2019, <https://www.statista.com/topics/2333/e-commerce-in-the-united-kingdom/>, accessed 22 November 2019.
3. Alison Flood, 'Fake Books Sold on Amazon Could be Used for Money Laundering', *The Guardian*, 27 April 2018.
4. Author interview with payment-processing company B, London, 2 July 2019.
5. Leonard L Gordon, 'Hanging Out to Dry: FTC's Ongoing Pursuit of Credit Card Laundering has Reached an Apex', Lexology, 14 December 2018, <https://www.lexology.com/library/detail.aspx?g=3abf1c9e-4dfb-416c-8d71-c7c37a179d60>, accessed 23 October 2019.

– such as online gambling or cryptocurrency – where instances of criminal exploitation have prompted a reappraisal of their anti-money-laundering/counter-terrorist-financing (AML/CTF) standards.[6]

In a similar vein, there is no doubt that fake or mispriced transactions through online marketplaces can be used as a pretext for moving funds, as demonstrated by the case of a terrorist sympathiser who received money under the cover of selling printers online.[7] There are, however, encouraging indications that online marketplaces are aware of their opportunities to detect such behaviour, such as a press report that the recent rise in the number of 'defence against money laundering' suspicious activity reports (SARs) filed in the UK may be attributable to e-commerce businesses such as Amazon Pay and Airbnb.[8] But, unlike the case of VAT fraud – which was the subject of a House of Commons hearing in 2017[9] – there has been no examination of the effectiveness of online marketplaces' defences against financial crime.

Against this background, this paper makes the following recommendations:

1. The Financial Conduct Authority should consider a thematic review of risks related to transaction laundering and financial institutions' ability to detect it, with a view to identifying best practices.
2. The National Crime Agency should consider arrangements for law enforcement engagement with payment processors and e-commerce marketplaces in order to share information on typologies and criminal trends.
3. In the context of the development of new e-commerce rules in the UK and the EU,[10] HM Government and the European Commission, respectively, should take account of financial crime risks along with more well-known threats such as counterfeit trade, drug trafficking or VAT fraud. In doing so, they should address the role of both online marketplaces and AML/CTF-regulated financial institutions involved in processing related payments.

---

6. See Anton Moiseienko and Kayla Izenman, 'From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency', *RUSI Occasional Papers* (September 2019); Anton Moiseienko, 'Play Your Cards Right: Preventing Criminal Abuse of Online Gambling', *RUSI Occasional Papers* (November 2019).
7. US vs. Mohamed Elshinawy, 'Memorandum Opinion', US District Court for the District of Maryland, 28 March 2018, p. 18.
8. Koos Couvée, 'Fintechs Fuel Surge in UK Defense Against Money Laundering Requests', Association of Certified Anti-Money Laundering Specialists (ACAMS), 17 October 2019, <https://www.moneylaundering.com/news/fintechs-fuel-surge-in-uk-defense-against-money-laundering-requests/?type=free>, accessed 23 October 2019.
9. House of Commons, Committee of Public Accounts, 'Tackling Online VAT Fraud and Error: First Report of Session 2017–19', 11 October 2017.
10. Both the UK and the EU are expected to depart from the rules currently contained in the EU's Electronic Commerce Directive, as explained in this paper.

4. The Home Office and HM Treasury should ensure that the UK's next national risk assessment of money laundering and terrorist financing addresses the risks of phantom transactions and mispricing involving online marketplaces. This should involve engagement with major online marketplaces used by UK customers to better understand the scale of the problem and measures taken to mitigate it.

Introduction

THE SALE OF goods and services online, known as e-commerce, has reached an enormous scale. According to the UN Conference on Trade and Development (UNCTAD), it amounted to $29 trillion in 2017, with business-to-consumer sales accounting for $3.8 trillion and 1.3 billion people shopping online.[1] Another estimate forecasts the growth in business-to-consumer sales to $5.8 trillion by 2022.[2] In the UK alone, the volume of e-commerce sales in 2017 was estimated at $586 billion.[3]

As the current experience of the financial system and international trade suggests, the larger the scale of legitimate commercial activities, the greater the opportunity to conceal criminal transactions under their guise. From the sale of fake books on Amazon[4] to 'ghost rides' on Uber and Lyft[5] and stays on Airbnb,[6] diverse means can be employed to move criminally obtained funds.

In addition to the sheer scale of e-commerce, the challenges of countering financial crime (that is, money laundering and terrorist financing) in the sector are compounded by the diversity of actors involved, ranging from e-commerce merchants to financial institutions involved in processing payments.

---

1. United Nations Conference on Trade and Development (UNCTAD), 'Global E-Commerce Sales Surged to $29 Trillion', 29 March 2019, <https://unctad.org/en/pages/PressRelease.aspx?OriginalVersionID=505>, accessed 23 October 2019.
2. Jordan McKee, 'Global Digital Commerce Sales to Near $6 Trillion by 2022', *Forbes*, 11 September 2018.
3. S O'Dea, 'E-Commerce in the United Kingdom (UK) – Statistics & Facts', 31 July 2019, <https://www.statista.com/topics/2333/e-commerce-in-the-united-kingdom/>, accessed 22 November 2019.
4. Alison Flood, 'Fake Books Sold on Amazon Could be Used for Money Laundering', *The Guardian*, 27 April 2018.
5. Ron Teicher, 'How Uber Ghost Rides are Linked to Online Money Laundering', *The Next Web*, 18 March 2018, <https://thenextweb.com/contributors/2018/03/18/uber-ghost-rides-linked-online-money-laundering/>, accessed 23 October 2019; 11Alive, 'Uber and Lyft Accounts Hacked in Money Laundering Scheme', 10 February 2019, <https://www.youtube.com/watch?v=fMzXNsvDZnQ>, accessed 23 October 2019.
6. Joseph Cox, 'Inside Airbnb's Russian Money-Laundering Problem', *Daily Beast*, 27 November 2017, <https://www.thedailybeast.com/inside-airbnbs-russian-money-laundering-problem?ref=scroll>, accessed 23 October 2019.

Against this background, this paper outlines the main financial crime risks inherent in e-commerce and suggests priority measures for their mitigation. It discusses four main categories of criminal exploitation:

- Committing fraud against the customer by failing to deliver goods or services.
- Buying goods or services using stolen bank card data.
- Creating e-commerce businesses as a front for illicit transactions.
- Abusing online marketplaces to move criminally obtained funds.

This paper forms part of RUSI's Financial Crime 2.0 research programme, which reviews financial crime vulnerabilities across the online economy, including in cryptocurrency businesses,[7] online games[8] and online gambling.[9] Compared to research on cryptocurrency and online gambling, the work on this paper has presented notable methodological challenges due to limited interview access. The author conducted three interviews with anti-money-laundering/counter-terrorist-financing (AML/CTF) compliance experts working for payment service providers servicing e-commerce businesses, and two interviews with experienced AML/CTF technology consultants advising e-commerce merchants. Despite five interview requests, no interviews were secured with major online marketplaces or payment scheme providers, while representatives of the two banks approached stated their institutions had no relevant expertise. One law enforcement agency has responded to the researcher's questions in writing.

This lack of access may be indicative of businesses' limited willingness to interact with research, but it should not be interpreted as an indicator of their indifference to crime prevention. In fact, some e-commerce companies appear to be contributing information to law enforcement, as suggested by occasional public-source references to suspicious activity reporting by Amazon, which are mentioned in this paper. It must also be noted that, while this study formed part of a larger project encompassing four sectors of the online economy, it is possible that a more in-depth examination of e-commerce businesses specifically would yield greater industry engagement.

As a result, this paper contributes to existing research by bringing together publicly available information – such as that gleaned from industry reports, court cases and news items – with a view to identifying key issues that policymakers should address. Although exploratory in nature, this analysis intends to add to the current understanding of financial crime risks related to e-commerce. Thus, it is expected to be of help to policymakers, law enforcement agencies and private sector professionals working in this area.

7. Anton Moiseienko and Kayla Izenman, 'From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency', *RUSI Occasional Papers* (September 2019).
8. Anton Moiseienko and Kayla Izenman, 'Gaming the System: Money Laundering Through Online Games', *RUSI Newsbrief*, 11 October 2019.
9. Anton Moiseienko, 'Play Your Cards Right: Preventing Criminal Abuse of Online Gambling', *RUSI Occasional Papers* (November 2019).

I. Financial Crime Risks in E-Commerce

TO SET THE stage for a discussion of possible responses, this chapter reviews the main financial crime risks inherent in e-commerce: e-commerce fraud; use of stolen bank cards for online purchases; e-commerce businesses being used as a front for illicit transactions; and e-commerce platforms being exploited to move criminal proceeds. Strictly speaking, except for the last instance, these modi operandi involve the generation of criminal proceeds, which then leads to money laundering when the proceeds are used.

E-Commerce Fraud

Given the physical distance between the buyer and seller, e-commerce transactions entail elevated fraud risks:

- Goods or services may not be delivered or may fall short of agreed specifications. The latter risk is particularly pronounced in relation to products whose quality cannot be easily ascertained by a lay customer, such as food supplements or medications.[10]
- Misleading information on the seller's website can lead to a customer unwittingly authorising repeat fund withdrawals from his or her bank account. In 2012, for example, the US Federal Trade Commission (FTC) entered a settlement with a businessman whose companies collected $359 million through deceptive charges for 'free trials' of products.[11]

In these instances, e-commerce businesses are used as a vehicle to perpetrate fraud and earn criminal income, rather than launder it. But once this income is deposited with a financial

10. For an example, see FBI, 'Scams and Safety: Common Fraud Schemes – Counterfeit Prescription Drugs', <https://www.fbi.gov/scams-and-safety/common-fraud-schemes/counterfeit-prescription-drugs>, accessed 23 October 2019. The quality of medicines purchased through unlicensed online pharmacies differs widely. See Brian Krebs, *Spam Nation: The Inside Story of Organized Cybercrime – From Global Epidemic to Your Front Door* (Naperville, IL: Sourcebooks, 2014), pp. 67–84.
11. Federal Trade Commission (FTC), 'FTC Halts Deceptive Practices of Marketer Who Collected $359 Million Using Bogus "Free" Trial Offers', press release, 23 February 2012, <https://www.ftc.gov/news-events/press-releases/2012/02/ftc-halts-deceptive-practices-marketer-who-collected-359-million>, accessed 23 October 2019. For a more recent case concerning similar practices, see FTC vs. Apex Capital Group, LLC et al., 'Complaint for Permanent Injunction and Other Equitable Relief', California Central District Court, 2:18-cv-09573, 14 November 2018.

institution or transferred elsewhere, a money-laundering offence takes place. Thus, financial institutions need to ascertain that they are not servicing fraudulent businesses.[12]

Use of Stolen Bank Cards

The use of stolen bank cards (also known as 'card-not-present fraud') is a risk common to all types of businesses that sell goods or services online, including cryptocurrency businesses, online gambling operators and online games.[13] Other sectors are also vulnerable – for instance, flight[14] and railway[15] tickets are known to have been booked using compromised cards. According to UK Finance, a trade association for UK financial institutions, fraudulent card purchases from UK retailers amounted to £265.1 million in 2018, mainly resulting from stolen card information obtained in data breaches.[16]

The problem is well known, and law enforcement agencies have had some success stories. In October and November 2019, a Europol-coordinated operation in 19 countries led to the arrest of 60 people suspected of involvement in over 6,500 fraudulent transactions, which allegedly generated €5 million in profit.[17] In the UK, the Dedicated Card and Payment Crime Unit (DCPCU), a specialist unit within the City of London Police, estimated that it had prevented £94.5 million of fraud, disrupted 11 organised crime groups and secured 48 convictions in 2018.[18]

The use of stolen bank cards is symbiotically linked to data breaches. Since criminals who perpetrate data breaches often gain more personal data than they alone can exploit, they sell

12. Money laundering is typically broadly defined. For instance, Article 6 of the UN Convention against Transnational Organized Crime defines money laundering as, among other things, the 'conversion' or 'transfer' of criminally derived property. This provision is referred to in the Recommendations of the Financial Action Task Force, the global standard-setter that informs countries' financial crime legislation.
13. For a discussion of the contrast in how some cryptocurrency businesses prevent the use of stolen cards in comparison to online gambling businesses, see Moiseienko, 'Play Your Cards Right', pp. 16–18. See also Moiseienko and Izenman, 'From Intention to Action'.
14. Europol, '79 Arrested in Worldwide Crackdown on Airline Fraud', press release, 27 November 2019, <https://www.europol.europa.eu/newsroom/news/79-arrested-in-worldwide-crackdown-airline-fraud> accessed 9 December 2019; Alice Hutchings, 'Flying in Cyberspace: Policing Global Travel Fraud', *Policing: A Journal of Policy and Practice*, 10 September 2018, pp. 1–16.
15. Europol, '60 E-Commerce Fraudsters Busted During International Operation', press release, 30 October 2019, <https://www.europol.europa.eu/newsroom/news/60-e-commerce-fraudsters-busted-during-international-operation>, accessed 26 November 2019.
16. UK Finance, 'Fraud: The Facts 2019', 2019, p. 15.
17. Europol, '60 E-Commerce Fraudsters Busted During International Operation'.
18. Glyn Whittick, 'DCPCU Prevents £94.5 Million of Fraud', UK Finance, 21 February 2019, <https://www.ukfinance.org.uk/news-and-insight/blogs/dcpcu-prevents-94-million-fraud>, accessed 26 November 2019.

all or part of it on cybercriminal forums.[19] Noting this, Europol characterises card-not-present fraud as the second-highest cybercrime law enforcement priority after ransomware, citing the example of the Marriott International breach in 2018, which resulted in the disclosure of over 300 million user records (albeit encrypted)[20] and a £99-million fine imposed on Marriott International by the UK's Information Commissioner's Office.[21] In some instances, criminals may set up their own e-commerce merchants to 'buy' goods or services using stolen credit cards, and then disappear before the funds can be recovered.[22]

Law enforcement agencies, such as London's Metropolitan Police Service, have published advice for businesses on how to minimise risks of card-not-present fraud, such as verifying the delivery address.[23] Ultimately, however, it is financial institutions who typically reimburse customers for fraudulent withdrawals from their accounts, which may create a moral hazard for some e-commerce businesses since they do not shoulder the losses.[24]

E-Commerce Front Companies

Some businesses can only access banking services through deception. This typically applies to businesses that undertake obviously illicit activities, such as the sale of unlawful narcotics, but can also happen with legitimate entrepreneurs deemed to pose high financial crime risks. The concealment of a company's genuine activities to obtain access to financial services is often known as 'transaction laundering'.

Unlike e-commerce fraud, transaction laundering generally masks consensual illegal transactions. For instance, a UK-based payment-processing company interviewed for this research discovered that one of its customers, ostensibly an art trading company, was selling illegal drugs online.[25] G2, a technology consulting company, describes a website that sold drugs under the guise of

19. For an up-to-date overview of criminal dark-web marketplaces, see European Monitoring Centre for Drugs and Drug Addiction and Europol*, EU Drug Markets Report* (Luxembourg: Publications Office of the European Union, 2019), pp. 68–69.
20. Europol, 'Internet Organised Crime Threat Assessment (IOCTA) 2019', 2019, p. 19.
21. Information Commissioner's Office, 'Statement: Intention to Fine Marriott International, Inc More Than £99 Million Under GDPR for Data Breach', 9 July 2019, <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/>, accessed 26 November 2019.
22. ThreatMetrix, 'ThreatMetrix Helps North American Bancard Identify and Block Fraudulent New Account Creations', 2017, <https://www.threatmetrix.com/digital-identity-insight/case-study/north-american-bancard/>, accessed 23 October 2019. This was also confirmed by law enforcement officer A, email to the author, 22 November 2019, although this typology was said to be 'not very frequent'.
23. Metropolitan Police Service, *The Little Book of Big Scams* (London: Mayor's Office for Policing and Crime, 2018), pp. 30–31.
24. The author is grateful to a reviewer for pointing this out.
25. Author interview with payment-processing company B, London, 2 July 2019.

clothes, with customers using codewords such as 't-shirt size' to indicate the type and quantity of drugs they required.[26] The use of this criminal typology, including in the context of drug sales, was confirmed by the law enforcement officer who shared their and their colleagues' observations with the author.[27]

The provision of illicit services may likewise require access to the payment infrastructure. RUSI's research on cybercrime suggests that criminals providing distributed denial-of-service (DDoS) attacks as a service incorporate companies and create fake websites to obtain payment facilities,[28] while another academic paper shows that the availability of diverse payment means affects the popularity of DDoS services.[29] In the US, transaction laundering has been employed by illicit online gambling operators.[30]

In detecting transaction laundering, test purchases through a company's website are a useful technique.[31] They are not, however, a silver bullet: transaction laundering can also involve a functioning legitimate business in a scheme sometimes known as 'unauthorised aggregation'.[32] For example, one criminal group set up a legitimate fundraising website, but its bank account was also used to collect payments from a network of illicit websites selling extreme pornography.[33] Furthermore, a legitimate company can choose to allow an illegitimate or high-risk business to direct payments through its merchant account in exchange for a fee.[34]

On the 'legitimate' side of the spectrum, a representative for a UK-based payment processor reported discovering that some customers were surreptitiously engaged in cryptocurrency exchange.[35] Some of them misrepresented the nature of their activities, not because these were illegal, but because these activities might be deemed high risk by the payment processor. The legitimate nature of the underlying business does not, however, alter the possibility that

26. Verisk Financial and G2, 'Transaction Laundering: Real Life Launderers', undated, p. 2.
27. Law enforcement officer A, email to the author, 22 November 2019.
28. Anton Moiseienko and Olivier Kraft, 'From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime', *RUSI Occasional Papers* (November 2018), p. 42.
29. Alice Hutchings and Richard Clayton, 'Exploring the Provision of Online Booter Services', *Deviant Behavior* (Vol. 37, No. 10, 2016), pp. 1163–78.
30. 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; Alasdair Pal, 'Exclusive: Fake Online Stores Reveal Gamblers' Shadow Banking System', *Reuters*, 22 June 2017.
31. Author interview with payment-processing company B, London, 2 July 2019.
32. Kasturi Chattopadhyay, *Transaction Laundering – A Growing Threat in the Payments Industry* (Bengaluru, India: Infosys, 2018), p. 2.
33. EverCompliant, 'Online Transaction Laundering and the Evolving Landscape of E-Commerce Merchant Fraud', July 2015, p. 6.
34. FTC vs. PayBasics, Inc et al., 'Complaint for Permanent Injunction and Other Equitable Relief', US District Court for the Northern District of Illinois, 15-cv-10963, 7 December 2015, para. 12.
35. Author interview with payment-processing company B, London, 2 July 2019.

the customer may be committing fraud against the bank or payment processor by mis-stating their activities.

Abuse of E-Commerce Platforms

Some of today's most successful online businesses operate as platforms that bring together buyers and sellers of goods or services. As is evident from the examples involving Amazon, Airbnb, Uber and Lyft,[36] criminals can use phantom transactions on such platforms to move value.

For instance, if Alice wants to send crime proceeds overseas to Bob, she may 'buy' non-existent goods or services from Bob through an online marketplace and pay him via one of the payment means supported by the platform in question. In effect, Alice and Bob engage in internet-enabled trade-based money laundering.[37]

This money-laundering typology resembles peer-to-peer interactions that can take place in online gambling, such as a deliberate 'loss' to an accomplice in an internet poker room, or online games, such as in-game transfers of valuable in-game items.[38] But while online games and most forms of gambling can exist without peer-to-peer financial interactions, peer-to-peer sales are indispensable for e-commerce platforms.

In this example, the illusion of a legitimate online business provides Bob with a plausible explanation as to why he is in receipt of the money. But unless Alice can pay in cash, which is unlikely to be practical at a great distance, she must first place her criminally obtained income in a bank account. This is the first hurdle to overcome in order to make use of this money-laundering scheme.

By providing an ostensibly legitimate reason for a payment, overpricing and phantom transactions can facilitate terrorist financing. In 2015, a US criminal complaint detailed how an American suspect received at least $1,200 from a member of Daesh (also known as the Islamic State of Iraq and Syria, ISIS) through PayPal under the pretext of selling printers on eBay.[39] The suspect pleaded guilty and was sentenced to 20 years' imprisonment in 2018.[40]

---

36. Teicher, 'How Uber Ghost Rides are Linked to Online Money Laundering'; 11Alive, 'Uber and Lyft Accounts Hacked in Money Laundering Scheme'; Cox, 'Inside Airbnb's Russian Money-Laundering Problem'.
37. Trade-based money laundering is explained in John Cassara, *Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement* (Hoboken, NJ: Wiley, 2016). See also Rena S Miller, Liana W Rosen and James K Jackson, 'Trade-Based Money Laundering: Overview and Policy Issues', Congressional Research Service, CRS Report, 22 June 2016.
38. See examples in Moiseienko, 'Play Your Cards Right' and Moiseienko and Izenman, 'Gaming the System'.
39. US vs. Elshinawy, 'Memorandum Opinion', p. 18.
40. Wyre Davies, 'The Global Terror Network That Started in Pontypridd', *BBC News*, 16 July 2018.

Furthermore, a similar technique could be used for sanctions evasion (namely, to transfer value to persons subject to financial sanctions). This is demonstrated by the $466,912 settlement with Apple that the US Office of Foreign Assets Control (OFAC) announced in November 2019. The settlement related to over $1 million in payments for software applications that a Slovenian software company, SIS d.o.o., was offering to customers through Apple's App Store. The company has been subject to US sanctions under the Foreign Narcotics Kingpin Designation Act since February 2015, on the grounds that it is under the control of an individual whom the US government believes to be involved in drug trafficking. According to the designation, the individual's 14 companies, including SIS d.o.o., 'receive payments from … steroid sales as part of the organization's laundering of illicit proceeds and for the purchase of assets worldwide'.[41] Due to deficiencies of its sanctions-screening system, Apple failed to establish that SIS d.o.o. was subject to sanctions, with the following result:

> Apple continued to host software applications and associated content ('apps') owned by SIS on the App Store, allowed downloads and sales of the blocked SIS apps, received payments from App Store users downloading the blocked SIS apps, permitted SIS to transfer and sell its apps to two other developers, and remitted funds on a monthly basis to SIS for the sales of the blocked SIS apps.[42]

OFAC's announcement does not, however, state that any of the customers' payments for SIS d.o.o. apps were payments for drug supplies. Therefore, if OFAC's allegations of drug trafficking are well founded,[43] SIS d.o.o. may have been a legitimate arm of an otherwise criminal business empire. But its activities could equally have been used to move funds or accept payments for drug supplies under the pretence of legitimate commerce.

Apart from phantom sales or mispricing, it is also possible for criminals to use e-commerce platforms to sell goods that were stolen or otherwise criminally obtained. For instance, Michael McGuire cites a conversation on a cybercriminal forum where one participant suggested purchasing gold using criminal income and then reselling it on eBay.[44]

Finally, some marketplaces are created to facilitate illegal activity, such as cybercrime or trade in counterfeit products. For instance, the EU Intellectual Property Office (EUIPO) and Europol cite a Europol-coordinated operation against 'an illegal online marketplace containing 10,000 shops

41. US Department of the Treasury, 'Treasury Sanctions Network of Slovenian Steroid Trafficker Mihael Karner', press release, 24 February 2015, <https://www.treasury.gov/press-center/press-releases/Pages/jl9980.aspx>, accessed 9 December 2019.
42. US Office of Foreign Assets Control (OFAC), 'Enforcement Information for November 25, 2019', <https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20191125_apple.pdf>, accessed 26 November 2019.
43. It is important to note that financial sanctions are imposed extra-judicially and the underlying allegations are rarely tested in court.
44. Michael McGuire, 'Into the Web of Profit: Understanding the Growth of the Cybercrime Economy', Bromium, April 2018, p. 89.

selling anything you could imagine', resulting in 100 prosecutions.[45] Since such marketplaces are criminal by design and thus not amenable to regulation, they are beyond the scope of this paper. It is, however, worth noting that the EUIPO and Europol highlight the trend towards increased sales of counterfeit products via social media and, in some instances, mobile instant messaging platforms.[46]

45. EU Intellectual Property Office (EUIPO) and Europol, 'Intellectual Property Crime Threat Assessment 2019', 2019, p. 37.
46. *Ibid*., pp. 26, 37.

II. Actors Involved and Their Responses

IN THE AFOREMENTIONED scenarios, e-commerce businesses are either operated by criminals for nefarious purposes or, in the case of online marketplaces, unwittingly abused to move criminal proceeds. But e-commerce involves a range of actors beyond businesses themselves. Financial institutions process payments from customers and, for physical goods, delivery services can be used. The following chapter discusses the role played by each of these actors in mitigating the financial crime risks of e-commerce.

Financial Institutions

To discuss the role of financial institutions in detecting and preventing financial crime related to e-commerce, it is helpful to begin with their functions in e-commerce payments.

Table 1: Institutions Typically Involved in E-Commerce Payments.

Institution	Function
Issuing bank	Issues the buyer's credit or debit card used to make the payment.
Payment gateway company	Processes payment requests for the e-commerce merchant's website, conducts limited anti-fraud checks* and directs payment requests to the merchant acquirer.
Merchant acquirer (also known as *acquiring bank*)	Acts as the bank where the merchant (seller) holds the account it uses to receive payments (known as *merchant account*). The income held in the *merchant account* is regularly transferred to the merchant's *current account*, which may be held with another bank.
Payment scheme (for example, Visa or MasterCard)**	Enables the merchant acquirer to request the payment from the buyer's issuing bank.
Seller's bank	Provides the merchant with a *current account*. This may or may not be the same bank as the merchant acquirer, where the *merchant account* is held.

Institution	Function
Payment processors (for example, PayPal)	Some merchants choose to use payment processors, such as PayPal or Skrill, which receive the payments on the merchant's behalf and deposit the proceeds, minus their fee, to the merchant's *current account*. A payment processor therefore removes the need for the merchant to have its own *merchant account* and payment gateway.

** Limited anti-fraud checks include, for example, checking the address indicated by the customer against the address held by the bank that issued the card. See John Solomon, 'How Payment Gateways Can Detect and Prevent Online Fraud', Chargebee, undated, <https://www.chargebee.com/blog/optimize-online-billing-stop-online-fraud/>, accessed 23 October 2019.*

*** While Visa and MasterCard are the best-known payment schemes in the UK, there are several other notable payment schemes internationally, such as American Express, Discover and UnionPay.*

Source: BarclayCard, 'How Do Online Payments Actually Work?', undated, <https://www.barclaycard.co.uk/business/accepting-payments/learn-about-taking-payments/how-do-online-payments-actually-work>, accessed 23 October 2019.

Banks and Payment Processors

As shown in Table 1, several AML/CTF-regulated financial institutions may be involved, including a payment processor and up to three banks: the bank that issued the buyer's card; the merchant acquirer used by the seller; and the bank where the seller holds its current account. In line with AML/CTF regulations,[47] these institutions are obliged to conduct customer due diligence and file suspicious activity reports (SARs).[48] If the goods or services that are being bought or sold

47. Domestic AML/CTF legislation is typically based on the recommendations published by the Financial Action Task Force (FATF), which are not legally binding but widely accepted in practice. See FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', 2012 (last updated June 2019). EU member states are bound by 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', L 141/73, *Official Journal of the European Union* (London: The Stationery Office, 2015) (4th Money Laundering Directive).
48. In the UK, for instance, the application of the full spectrum of AML/CTF requirements to merchant acquirers is confirmed by the Joint Money Laundering Steering Group, 'Guidance for the UK Financial Sector: Part II', December 2017, pp. 32, 35, <http://www.jmlsg.org.uk/news/jmlsg-revised-guidance>, accessed 23 October 2019.

are unusual in view of the customer's profile, a red flag should be raised, and further enquiry may be warranted.[49]

The insight that banks and payment processors have into customers' activities can vary. For instance, the merchant acquirer will only see the customers' e-commerce revenues, but not the rest of their financial activities. The fragmented picture that financial institutions have of the customer's activity is a well-known constraint on the ability to detect financial crime, and one that is by no means unique to e-commerce.[50] Another key consideration – particularly in the context of payment processors, of which there is a great number and variety – is the consistency of AML/CTF standards across institutions.[51]

While e-commerce fraud is likely to generate customer complaints and chargebacks, this is not true of transaction laundering. In the absence of obvious incongruities, its detection is challenging. According to two payment-processing companies, red flags include:

- Pricing that is incongruent with the goods being sold.
- The sale of intangible goods that are difficult to value.
- Customers' attempts to conceal identity or location, such as through a VPN.[52]
- Unusual counterparties, such as an electronics company making payments to an individual.[53]

Test purchases are helpful, but if a functioning legitimate business is used as a cover for illicit transactions, they are likely to be of limited effect. A fuller investigation may be necessary, which will typically involve the use of both public-source data and proprietary databases to establish connections between websites, businesses and the individuals in charge of them.[54] Measures taken to detect transaction laundering include 'web content monitoring, making use of SEO [search engine optimisation] analytics tools, doing test transactions or manually searching on Google etc'.[55]

But in the absence of best-practice guidance by regulators, it is unclear how far financial institutions should go in verifying the genuine nature of their customers' business, or the extent to which a greater availability of intelligence on transaction laundering would benefit

49. Wolfsberg Group, 'Wolfsberg AML Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities', 2009, p. 9.
50. Matthew Redhead, 'Deep Impact? Refocusing the Anti-Money Laundering Model on Evidence and Outcomes', *RUSI Occasional Papers* (October 2019), p. 20.
51. Michael Levi, 'Money Laundering Risks and E-Gaming: A European Overview and Assessment', European Gaming and Betting Association, September 2009, pp. 15–16.
52. Author interview with payment-processing company B, London, 2 July 2019.
53. Author interview with payment-processing company A, London, 14 June 2019.
54. Author telephone interview with technology consultant B, 17 April 2019.
55. Brandon Li, 'Transaction Laundering in 2019 – Time to Review the Monitoring Strategy', The Paypers, 8 January 2019, <https://thepaypers.com/expert-opinion/transaction-laundering-in-2019-time-to-review-the-monitoring-strategy/776727>, accessed 9 December 2019.

law enforcement. Both payment processors interviewed for this research expressed concern that they were not aware of law enforcement priorities, nor did they have any indications of how useful their SARs were.[56] To a degree, this can be rectified by establishing a forum for the sharing of typologies and trends between law enforcement agencies, payment service providers and major e-commerce marketplaces. However, businesses should aim to ensure that their efforts at preventing criminal activity reflect their own understanding of the risks they face, which can be superior to that of law enforcement agencies in some respects.[57]

To date, there appears to be no evidence of a regulatory or law enforcement focus on transaction laundering in the UK. The situation is different in the US. Since 2016, the FTC has brought several cases against payment processors for knowingly facilitating transaction laundering, with one of the settlements involving $280.9 million.[58] It is likely that the US focus on transaction laundering is a consequence of the fact that the Telemarketing and Consumer Fraud and Abuse Prevention Act, which was adopted in 1994, explicitly required the FTC to promulgate rules addressing 'credit card laundering', which it did in 1995.[59] As with other regulated sectors, however, enforcement against those who wittingly flout AML/CTF regulation can and should be usefully complemented by the education of those who wish to do the right thing but may be deceived by criminals.[60]

Regarding the abuse of e-commerce platforms, it is particularly difficult for financial institutions to identify phantom sales or mispricing. Abnormal prices constitute a red flag, as in the case of books trading at thousands of pounds apiece. For instance, the Association of Certified Financial Crime Specialists lists the questions that should be asked to identify phantom shipments:

- Do the transactions make sense in terms of amounts, customers or items being sold?
- Why is the buyer going international when they could get the same items domestically?
- Is there any hard evidence that, even though a payment was made, an item was actually shipped?[61]

56. Author interview with payment-processing company A, London, 14 June 2019; author interview with payment-processing company B, London, 2 July 2019.
57. The author is grateful to a reviewer for this point.
58. For an overview, see Leonard L Gordon, 'Hanging Out to Dry: FTC's Ongoing Pursuit of Credit Card Laundering has Reached an Apex', Lexology, 14 December 2018, <https://www.lexology.com/library/detail.aspx?g=3abf1c9e-4dfb-416c-8d71-c7c37a179d60>, accessed 23 October 2019.
59. Telemarketing and Consumer Fraud & Abuse Prevention Act 1994, Section 3(2). See also the Telemarketing Sales Rule, 16 CFR Part 310.3(c).
60. For this argument, in the context of both financial and non-financial businesses, see David Artingstall, 'Examining the Unknowns: Money-Laundering Risk in the UK Professional Services Sectors – Threats and Responses', *RUSI Occasional Papers* (June 2019), p. 22.
61. Association of Certified Financial Crime Specialists, 'Merchant-Based Money Laundering Part 1: Phantom Shipments', 8 September 2016, <https://www.acfcs.org/merchant-based-money-laundering-part-1-phantom-shipments/>, accessed 9 December 2019.

Obvious irregularities aside, it is challenging to detect mispricing. According to one interviewee, mispricing is particularly common in respect of high-volume, moderate-value goods whose pricing varies significantly depending on commercial conditions.[62] This is a familiar challenge in the context of trade-based money laundering. Recognising this, the joint guidance produced by the Wolfsberg Group, the International Chamber of Commerce and the Bankers Association for Finance and Trade states:

> Even in transactions involving regularly traded commodities, which are subject to publicly available market prices, [financial institutions] generally are not in a position to make meaningful determinations about the legitimacy of unit pricing due to the lack of relevant business information, such as the terms of a business relationship, volume discounting or the specific quality of the goods involved … However, there may be situations where unit pricing appears manifestly unusual.[63]

Furthermore, in most cases neither online marketplaces nor financial institutions involved can reliably ascertain whether a shipment has taken place. They can and do request bills of lading or proof of sending, but these can be forged with relative ease and, at any rate, such requests are reserved for cases where red flags have already been raised.[64]

Information obtained from online marketplaces can be helpful in some instances, but according to an interviewee, it is the most established marketplaces like Amazon that tend to be most effective in detecting suspicious activities. They also have the most cooperation with payment processors, with less-known e-commerce platforms occasionally lagging behind.[65] Assuming that this observation is accurate, several factors could explain this difference. Among them are the fact that larger marketplaces may: run their own AML/CTF-regulated payment processors; be subject to greater transparency requirements if the marketplace is operated by a listed company that can face shareholder pressure to address risks related to criminal abuse;[66] and may have greater resources available to them.

Payment Schemes

Given their role, one might expect major payment schemes to have information on customer activity across accounts with multiple banks. However, according to a payment scheme representative, they do not collect transaction-level data and their AML/CTF efforts focus on

62. Author interview with payment-processing company A, London, 14 June 2019.
63. Wolfsberg Group, International Chamber of Commerce and Bankers Association for Finance and Trade, 'Trade Finance Principles: 2019 Amendment', 2019, p. 12.
64. Author interview with payment-processing company A, London, 14 June 2019.
65. Author interview with payment-processing company B, London, 2 July 2019.
66. For example, Amazon's 2018 annual report explicitly mentions the risks of it being held liable for 'fraudulent or unlawful activities of sellers'. See its submission to the US Securities and Exchange Commission, <https://www.sec.gov/Archives/edgar/data/1018724/000101872419000004/amzn-20181231x10k.htm>, accessed 26 November 2019.

ensuring that issuing and acquiring banks have proper AML/CTF controls in place.[67] As detailed in an article by Mark MacCarthy, the former Senior Vice President for Public Policy at Visa, payment schemes use three further techniques for detecting and preventing illicit behaviour:

- **MCC codes**. Each e-commerce merchant is required to indicate a four-digit merchant category code (MCC) identifying its main line of business. Some transactions, such as gambling-related ones, can be blocked on the basis of their MCC. Furthermore, high-risk MCCs can attract additional scrutiny from merchant acquirers or payment processors. To evade blocking or unwanted attention, criminals therefore have the incentive to incorrectly indicate low-risk MCCs.[68]
- **Manual checks**. Although it is the responsibility of merchant acquirers and payment processors to prevent the abuse of MCC codes, payment schemes occasionally check e-commerce websites to identify businesses' genuine areas of activity.[69] More broadly, they employ such checks to detect illicit activities by merchants that use the relevant payment scheme, such as sales of child pornography, controlled substances or counterfeit goods.
- **Accepting complaints**. In addition to their own controls, payment schemes react to complaints by affected businesses, such as IP rights holders whose rights are being infringed through illicit online sales.[70]

Payment schemes also incentivise fraud prevention by policing the chargeback rate – in other words, the rate at which a given merchant's customers request their banks to reimburse payments made to that merchant. Specifically, they impose penalties on merchant acquirers that serve businesses whose chargeback rate exceeds 1%.[71] In cases of collusion, criminals have been known to reimburse payment processors for penalties incurred.[72]

The issue of whether payment schemes should or can do more has been raised in the press,[73] and the answer depends on the schemes' ability to access individual-level transactions, which

67. Email from a payment scheme representative to the author, 17 April 2019. In the case of MasterCard and Visa, their requirements can be found in MasterCard, 'MasterCard Rules', 25 June 2019, pp. 29–30; Visa, 'Visa Core Rules and Visa Product and Service Rules', 13 April 2019, pp. 521–22.
68. Verisk Financial/G2, 'Transaction Laundering: Real Life Launderers', p. 9.
69. Mark MacCarthy, 'What Payment Intermediaries are Doing About Online Liability and Why It Matters', *Berkeley Technology Law Journal* (Vol. 25, No. 1037, 2010), pp. 1062–64.
70. *Ibid*., pp. 1090–98.
71. The Chargeback Company, 'Chargeback Ratio', 15 October 2018, <https://thechargebackcompany.com/chargeback-ratio/>, accessed 23 October 2019.
72. US vs. Gery Shalon et al., 'Sealed Superseding Indictment', New York Southern District Court, 15-cr-00333, 22 October 2015, paras. 32–33.
73. Andrew Ross Sorkin, 'How Banks Unwittingly Finance Mass Shootings', *New York Times*, 24 December 2018.

appears to be lacking at present.[74] If there is no such capacity at the moment, one may wonder whether its lack is an inevitable feature of the system or a deliberate technological choice that can be reversed if payment schemes so wished (or were required to do so by regulation).

Online Marketplaces

The role of online marketplaces in preventing criminal behaviour has already come to the fore in the context of counterfeit sales[75] and VAT fraud.[76] Legitimate marketplaces expressly prohibit the sale of illicit items, as well as of high-risk categories of goods, such as tobacco products.[77] They also take other measures against criminal misuse (for instance, by comparing listed goods against the database of registered trademarks).[78] In connection with VAT fraud, a 2017 hearing in the House of Commons' Committee of Public Accounts shed light on some measures taken by online marketplaces to detect and deter misuse, such as:

> Amazon maintained that it has processes in place, such as checking IP and legal addresses, to prevent fraudulent sellers that have been removed from its platform re-emerging under the banner of another company.[79]

Importantly, payments made on Amazon are processed by its AML/CTF-regulated payment subsidiary, Amazon Payments Europe S.C.A, a Luxembourg-registered e-money institution.[80] Depending on the data-sharing arrangements between Amazon group companies and applicable data-protection rules, one might expect this subsidiary to have more information about the activities taking place on the Amazon marketplace than unaffiliated payment processors have in relation to the e-commerce platforms they service. Interestingly, a press report from October

74. In the context of recent reports that MasterCard was selling information to Google, MasterCard emphasised that no individual transaction data was being provided, although it did not explicitly state that it was technologically impossible to provide such data. See Mark Bergen and Jennifer Surane, 'Google and MasterCard Cut a Secret Ad Deal to Track Retail Sales', *Bloomberg*, 30 August 2018.
75. Donald J Trump, 'Memorandum on Combating Trafficking in Counterfeit and Pirated Goods', 3 April 2019.
76. House of Commons, Committee of Public Accounts, 'Tackling Online VAT Fraud and Error: First Report of Session 2017–19', 11 October 2017.
77. Alexander Babuta, Cathy Haenlein and Alexandria Reid, 'E-Commerce, Delivery Services and the Illicit Tobacco Trade', *RUSI Occasional Papers* (October 2018), pp. 23–24.
78. Parminder Dyal and Stephen Lowry, 'Online Marketplaces Get Tough on Counterfeiters', Barker Brettell, 20 June 2019, <https://www.barkerbrettell.co.uk/online-marketplaces-get-tough-on-counterfeiters/>, accessed 9 December 2019.
79. House of Commons, Committee of Public Accounts, 'Tackling Online VAT Fraud and Error', p. 13.
80. Amazon Pay, 'Licence Information', <https://pay.amazon.co.uk/help/201751610>, accessed 23 October 2019. Note that the Amazon group also has a UK-based subsidiary, Amazon Payments UK Limited, which is regulated as an authorised payment institution. See FCA, 'The Financial Services Register', <https://register.fca.org.uk/>, accessed 23 October 2019.

2019 suggests that the rise in the number of 'defence against money laundering' SARs filed in the UK[81] could be attributable to e-commerce businesses, including Amazon Pay and Airbnb.[82] A further article speculates that Amazon Pay may be the e-money institution that, according to the 2018 annual report by Luxembourg's Financial Intelligence Unit (FIU),[83] was Luxembourg's largest filer of SARs and suspicious transaction reports (STRs).[84]

The sector's intelligence potential is also reflected in the fact that FIU.NET, the EU's network of FIUs, had run a project focused specifically on the sharing of SARs filed by major e-commerce platforms and payment processors:

> This project is associated with the ambiguous situation of several reporting entities registered and established in Luxembourg: PayPal, Amazon, and IPay. [T]hey are legally obliged to send their suspicious transactions reports (STRs) to the Luxembourg FIU, even if the transactions are related to other member states such as France and [the] UK. The pilot project was launched to require FIU Luxembourg to share spontaneously 'all STRs filed by Amazon, Paypal and Ipay with other national FIUs via the FIU.NET Crossborder system. 90 percent of cross-border reports were transferred to another FIU within 24 hours and 99 percent within 3 days'.[85]

The project contributes to the implementation of the EU's 4th Money Laundering Directive, which requires that '[w]hen an FIU receives a report … which concerns another Member State, it shall promptly forward it to the FIU of that Member State'.[86]

In the AML/CTF context, the kind of analysis cited by the Committee of Public Accounts could contribute to the identification of connected buyers and sellers, which may be indicative of money laundering or terrorist financing – for instance, when two ostensibly unrelated businesses that trade with each other are in fact accessed from the same IP address at the same

81. That is, SARs whereby the reporter requests the National Crime Agency to provide immunity for an act which could otherwise be prosecuted as money laundering.
82. Koos Couvée, 'Fintechs Fuel Surge in UK Defense Against Money Laundering Requests', ACAMS, 17 October 2019, <https://www.moneylaundering.com/news/fintechs-fuel-surge-in-uk-defense-against-money-laundering-requests/?type=free>, accessed 23 October 2019.
83. Cellule de Renseignement Financier (CRF), 'Rapport Annuel 2018', October 2019, p. 25, <https://justice.public.lu/dam-assets/fr/publications/rapport-activites-crf/rapport-crf-2018.pdf>, accessed 23 October 2019.
84. Gabriel Vedrenne, 'Amazon, PayPal Drove Significant Increase in Luxembourg SARs and STRs', ACAMS, 23 October 2019, <https://www.moneylaundering.com/news/amazon-paypal-drove-significant-increase-in-luxembourg-sars-and-strs/> accessed 9 December 2019. While different countries typically use the terms SAR and STR to denote the same type of reporting, Luxembourg's FIU distinguishes between STRs (which refer specifically to financial transactions) and SARs (which refer to any other category of suspicious behaviour). See CRF, 'Rapport Annuel 2018', p. 13.
85. European Parliament, 'Fighting Tax Crimes – Cooperation Between Financial Intelligence Units: Ex-Post Impact Assessment', March 2017, p. 70.
86. Article 53(1) of the 4th Money Laundering Directive.

time. Since online marketplaces are not subject to AML/CTF regulation per se, there appears to be no publicly available information on whether they do so or the extent to which such information is shared with law enforcement agencies or financial institutions (and, if it is being shared, in what way). Nor have there been any public hearings to explore the issue, unlike in relation to VAT fraud.

There has been recent movement towards rethinking crime prevention on online marketplaces, both in the UK and in the EU, although not in the context of anti-money laundering specifically. Up to now, EU states are constrained in their ability to deputise online marketplaces with detecting illicit activities. Article 15 of the Electronic Commerce Directive provides that:

> 1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
>
> 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.[87]

According to the UK government's *Online Harms White Paper*, this means, in effect, that e-commerce platforms are 'not liable for a piece of user-generated illegal content until they have received a notification of its existence, or if their technology has identified such content, and have subsequently failed to remove it from their services in good time'.[88] This is in line with the judgments of the Court of Justice of the EU, which ruled that EU law does not prevent governments from either requiring online marketplaces to remove content declared unlawful[89] (as long as this does not amount to a general obligation to identify illegal content) or issue injunctions to end intellectual property rights violations.[90]

The UK government's white paper did not refer to money laundering as one of the criminal risks involved, but announced its plans to introduce 'a new statutory duty of care' for e-commerce platforms, with its observance overseen by a new regulator.[91]

---

87. See 'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce)', *Official Journal of the European Communities* (L 178, 17 July 2000).
88. HM Government, *Online Harms White Paper*, CP 57 (London: The Stationery Office, 2019), p. 63.
89. Eva Glawischnig-Piesczek vs. Facebook Ireland Limited, 'Judgment of the Court (Third Chamber)', CJEU, C-18/18, 3 October 2019.
90. L'Oréal SA et al. vs. eBay International AG et al., 'Judgment of the Court (Grand Chamber)', CJEU, C-324/09, 12 July 2011.
91. HM Government, *Online Harms White Paper*, p. 7.

Furthermore, the applicability of the E-Commerce Directive in the UK will cease once the country leaves the EU,[92] while the new President of the European Commission, Ursula von der Leyen, has promised to amend the Directive through '[a] new Digital Services Act [that] will upgrade our liability and safety rules for digital platforms, services and products'.[93] With possible criminal misuse of e-commerce platforms at the fore of policymakers' minds in both the UK and EU, the time is ripe to ensure that financial crime considerations are part of the discussion.

92. HM Treasury, 'E-Commerce Directive Statement: Explanatory Information', <https://www.gov.uk/government/publications/onshoring-of-elements-of-the-e-commerce-directive-relating-to-financial-services/e-commerce-directive-statement-explanatory-information>, accessed 23 October 2019.
93. Ursula von der Leyen, 'A Union That Strives for More: My Agenda for Europe', 2019, p. 13, <https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf>, accessed 9 December 2019.

Conclusions and Recommendations

GIVEN THE SCALE of e-commerce, it is beyond doubt that some e-commerce transactions are exploited for money laundering and terrorist financing. As this paper has shown, there are multiple instances of criminal groups using e-commerce businesses to receive payments for illicit transactions, as well as at least one recorded case of fake e-commerce sales used as a pretext for terrorism-related money transfer.

In other sectors, such as online gambling or cryptocurrency, instances of criminal exploitation have prompted a reappraisal of their AML/CTF standards. The research for this paper, which is based predominantly on public-source information, has disclosed an apparent lack of a similar focus on financial crime in e-commerce, save for a series of FTC enforcement actions against complicit payment processors.

This dearth of attention contributes to an insufficient understanding of the parts that actors involved – including online marketplaces and payment schemes – can play in detecting and preventing financial crime in the sector. Together with the inherent difficulty of detecting consensual and possibly well-disguised transactions between criminal accomplices, financial crime through e-commerce is a younger cousin of trade-based money laundering; a set of techniques that are notoriously hard to tackle. A better understanding of the issue can inform further engagement with both online marketplaces and AML/CTF-regulated financial institutions involved in processing related payments, which sometimes are part of the same corporate group (as in the case of Amazon), but often are not.[94]

To pierce this veil of ignorance and take steps towards a better understanding of the financial crime vulnerabilities of e-commerce, this paper proposes the following priority measures:

- The Financial Conduct Authority should consider a thematic review of risks related to transaction laundering and financial institutions' ability to detect it, with a view to identifying best practices.
- The National Crime Agency should consider arrangements for law enforcement engagement with payment processors and major e-commerce marketplaces in order to share information on typologies and criminal trends.
- In the context of the development of new e-commerce rules in the UK and the EU, HM Government and the European Commission respectively should take account of financial crime risks along with more well-known threats such as counterfeit trade, drug trafficking

94. The need for such engagement was affirmed by law enforcement officer A, email to the author, 22 November 2019.

or VAT fraud. In doing so, they should address the role of both online marketplaces and AML/CTF-regulated financial institutions involved in processing related payments.

- The Home Office and HM Treasury should ensure that the UK's next national risk assessment of money laundering and terrorist financing addresses the risks of phantom transactions and mispricing involving online marketplaces.[95] This should involve engagement with major online marketplaces used by UK customers to better understand the scale of the problem and measures taken to mitigate it.

95. Under Regulation 16 of the Money Laundering Regulations 2017, the Home Office and HM Treasury must take steps to ensure the risk assessment remains up-to-date.

About the Author

Anton Moiseienko is a Research Fellow at RUSI's Centre for Financial Crime and Security Studies. His current and recent research covers a range of financial crime issues, including money laundering via online businesses, corruption in the UK and overseas, the intersection between cybercrime and money laundering, and financial crime risks posed by free trade zones.

Anton holds a PhD in Law from Queen Mary University of London and a Master's degree in Law from the University of Cambridge.