RUSI
Royal United Services Institute
for Defence and Security Studies

Emerging Insights

Following the Fraud: The Role of Money Mules

Kathryn Westmore and Allison Owen

July 2025

ACKNOWLEDGEMENTS

The authors thank the individuals who were interviewed for this paper, the peer reviewers who provided valuable comments that significantly improved this paper, and the RUSI Publications team. Lloyds Banking Group funded this research.

EXECUTIVE SUMMARY

Criminals are driven by profit, and in the past decade, fraud has proved to be one of the most profitable crimes. The high returns and low barriers to entry have opened up the market, allowing a range of actors to take advantage of the opportunities afforded to steal billions of pounds a year on a global basis. The UK has long been considered a 'target destination for fraudsters';[1] fraud accounts for over 40% of all crime in the UK,[2] and some estimates place the cost to the UK economy at more than £200 billion a year.[3] Furthermore, fraud causes significant emotional harm and distress to its victims. The scale and extent of fraud in the UK is so vast that it may reasonably be seen as a national security threat, undermining the rule of law and threatening the UK's financial sector.[4]

In particular, the rise of authorised push payment (APP) fraud has attracted considerable attention over the past decade. An APP fraud occurs when an individual is tricked into making a payment to a fraudster who they think is a genuine payee.[5] In many cases, they make a payment into an account operated by a so-called 'money mule' and controlled by the fraudster. This paper draws on transaction data, provided by Lloyds Bank, on the activity of known money mules, supplemented by a literature review and interviews with industry experts, to explore how funds are moved out of a money mule's account.

The paper's findings include:

- Newer entrants to the payments system, such as digital banks, payment firms and banking-as-a-service providers, receive a disproportionate share of transactions from known money mules compared with the

1. Helena Wood et al., 'The Silent Threat: The Impact of Fraud on UK National Security', *RUSI Occasional Papers* (January 2021), <https://www.rusi.org/explore-our-research/publications/occasional-papers/silent-threat-impact-fraud-uk-national-security>, accessed 24 June 2025.
2. HM Government, *Fraud Strategy: Stopping Scams and Protecting the Public*, CP 839 (London: The Stationery Office, 2023), p. 1.
3. Peters & Peters, 'Peters & Peters and Crowe Report Shows Fraud is Costing UK £219 Billion a Year', 26 July 2023, <https://www.petersandpeters.com/2023/07/26/what-is-the-cost-of-fraud-in-the-uk/>, accessed 15 May 2025.
4. HM Government, *Fraud Strategy*, p. 9.
5. Payment Systems Regulator (PSR), 'APP Scams', <https://www.psr.org.uk/our-work/app-scams/>, accessed 15 May 2025.

overall share of the payments they receive. One single firm received 20%, by value, of all the onward transfers via Faster Payments in the dataset. The increased fragmentation of the payments system has made it harder to track the flow of funds, and criminals appear to be able to exploit the relative weaknesses in the financial crime controls of these newer firms. This calls for a robust regulatory response.

- While most (57%) onward transfers are made via Faster Payments, a sizeable proportion of onward transactions are made with debit cards or through the withdrawal of cash. As banks and payment firms place stricter controls on customer onboarding and inward transaction monitoring, criminals may increasingly turn to methods other than bank transfers via Faster Payments to move money through the financial system. More research is needed to understand how this activity is changing and to manage the displacement risk.
- The range of destinations and ways of moving money from a money mule's account demonstrate the need to ensure that all parts of the payments ecosystem – including smaller payment firms and cryptocurrency services providers – are engaged in data-sharing initiatives to better prevent and detect fraud and the associated money laundering.
- Funds often only stay in a money mule's account for a short period of time, sometimes no more than 15 minutes. Acting fast is imperative. Closer collaboration between law enforcement and the private sector is crucial to real-time identification of frauds – which can allow fraudulent proceeds to be swiftly recovered and criminals to be arrested.

INTRODUCTION

Fraud is the crime that an individual is most likely to experience in the UK; it accounts for over 40% of all crime.[6] Scam texts, phishing emails, spoofed calls and fake adverts on social media – all designed to trick members of the public out of their money – bombard individuals every day. The Crime Survey of England and Wales (CSEW) estimates that there were 4.1 million incidents of fraud in England and Wales in the year ending December 2024.[7]

In recent years, there has been a greater focus on links between fraud and other types of crime – including organised crime, terrorist financing, proliferation financing, and human trafficking and modern slavery.[8] Previous RUSI research has found highly organised and widespread fraud attacks

6. HM Government, *Fraud Strategy,* p. 1.
7. Office for National Statistics, 'Crime in England and Wales: Year Ending December 2024', 24 April 2025, <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2024#fraud>, accessed 15 May 2025. Note that this records frauds committed against individuals.
8. Financial Action Task Force (FATF), Interpol and Egmont Group, 'Illicit Financial Flows from Cyber-Enabled Fraud', 9 November 2023, <https://www.fatf-gafi.org/

have the hallmarks of organised crime and are a threat to the UK's national security.[9] Fraud is increasingly acknowledged as a transnational problem; the National Crime Agency (NCA) estimates that over 75% of reported fraud is fully or partially committed overseas.[10]

The past decade has seen the emergence of authorised push payment (APP) frauds. These have attracted considerable attention.[11] An APP fraud occurs when an individual is tricked into making a payment to a fraudster who they think is a genuine payee.[12] At over £450 million in 2024,[13] the value of losses remains less than other types of fraud, such as card fraud. However, the devasting impact of APP fraud on victims and the scale of attacks have placed it firmly at the centre of the UK's fraud policy debate.[14] Furthermore, technology is making it ever easier for criminals to commit fraud; as lives have moved online, so have the fraudsters. Social media platforms have been widely identified as the origin for most frauds.[15] Fraudsters are now beginning to use new technologies, such as AI, to target victims more effectively and at scale.[16]

Money mules play a significant role in facilitating APP fraud. By providing criminals with accounts that can receive the proceeds of APP fraud and then rapidly moving those proceeds through the financial system, money mules allow fraudsters to obfuscate the flow of the funds. The public sector and industry have focused extensively on the role of money mules, including with the publication of a cross-system Money Mule and Financial Exploitation Action Plan in 2024.[17] However, a better and more nuanced understanding of how funds flow through the accounts of money mules – moving beyond simply identifying and closing money mule accounts – is essential in disrupting the ability of fraudsters to profit from their crimes.

---

en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html>, accessed 12 August 2024.

9. Wood et al., 'The Silent Threat'.
10. Supplementary Written Evidence Submitted by the NCA to the Home Affairs Select Committee on Fraud, 22 May 2024, <https://committees.parliament.uk/writtenevidence/130408/pdf/>, accessed 15 May 2025.
11. Kathryn Westmore, 'Fraud: The Emergence of a UK Epidemic', *RUSI Commentary*, 16 November 2023, <https://www.rusi.org/explore-our-research/publications/commentary/fraud-emergence-uk-epidemic>, accessed 15 May 2025.
12. PSR, 'APP Scams'.
13. UK Finance, 'Annual Fraud Report 2025', 28 May 2025, <https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2025>, accessed 30 May 2025.
14. HM Government, *Fraud Strategy*.
15. UK Finance, 'Annual Fraud Report 2025'.
16. PwC, 'Impact of Artificial Intelligence on Fraud and Scams', December 2023, <https://www.pwc.co.uk/services/forensic-services/insights/impact-of-artificial-intelligence-on-frauds-and-scams.html>, accessed 15 May 2025.
17. Home Office, 'Money Mule and Financial Exploitation Action Plan', 1 March 2024, <https://www.gov.uk/government/publications/money-mule-action-plan>, accessed 24 June 2025.

This research paper explores how criminal networks launder the proceeds of APP frauds that are committed in the UK onward. The ultimate aim of this work is to ensure that the current political focus on tackling fraud in the UK does not wane, and that policy, law enforcement and industry interventions are targeted to have the most disruptive impact possible on criminal networks and organisations.

METHODOLOGY

The term 'fraud' can mean many different things. The Fraud Act 2006 defines fraud as a dishonest act that is committed with a view to gain or with intent to cause loss or expose another to a risk of loss. It identifies three specific offences: dishonestly making a false representation; dishonestly failing to disclose information where there is a legal duty to disclose it; and dishonest abuse of position. Under the law, therefore, fraud can encompass a vast range of criminal activity. This paper is focused on one specific type of fraud by representation – APP fraud – although some contextual information is provided on fraud more generally.

The ultimate aim of this work is to ensure that the current political focus on tackling fraud in the UK does not wane

The methodology for this paper comprised three elements. First, a literature review of relevant academic and grey literature – including materials produced by the industry and evidence given to two UK parliamentary inquiries into the scope of fraud in the UK – was conducted. The literature review focused on the period 2016 to 2024; 2016 was chosen as the starting point because fraud-related questions were first included within the CSEW in that year. The literature review aimed to identify examples of methods used by criminals to launder the proceeds of APP frauds. A second phase of the literature review included an analysis of the various statistics relating to APP fraud in the UK. This included data from UK Finance, the Payment Systems Regulator (PSR), the Financial Conduct Authority (FCA), the Office for National Statistics and other industry participants – including banks, anti-fraud groups, non-profit organisations, blockchain analytics companies and other private sector entities.

Second, Lloyds Banking Group (Lloyds Bank) securely provided anonymised transaction and account data. This dataset included the volume of accounts that were identified as mule accounts, the age of each account and of the account holder, and the destination of the onward funds. Several discussions were held with individuals from the bank to clarify questions about the data and to validate the analysis performed by the research team. Finally, eight semi-structured interviews were carried out with experts in the field, including from law enforcement and industry. No interviews were conducted with representatives from Lloyds Bank. A clear caveat to the research methodology is that it draws on data from just one financial institution. There is therefore a risk of bias in the data analysis. Evidence from other sources – including the literature review and the interviews – has, where possible, been used to corroborate the findings from the transaction data, to mitigate this risk as far as possible. An analysis of data from one set of transactions at one financial institution is only a partial picture of transaction

flows. The assessment of the data in this paper should, therefore, be seen as a starting point for further research to explore the prevalence of the key trends identified in the data from Lloyds Bank within the broader ecosystem.

A TYPICAL APP FRAUD JOURNEY

APP frauds typically start outside the financial system, notably on online platforms or telecommunications services. Data from UK Finance shows that 70% of APP frauds in 2024 started on online platforms and these accounted for 29% of total losses. 16% of frauds started on telecommunications – either phone calls or SMS – and these accounted for 36% of losses.[18]

There are several types of APP fraud, but the 'scam journey' is similar. The scam may originate on social media, dating sites or online auction houses. The fraud victim may respond to an advert that they see or be contacted directly by a fraudster. Victims may also be targeted by a phone call or a text message, or – in a small number of cases – in person or by other means. The victim is then persuaded to transfer money from their account to an account controlled by a criminal, often a money mule who wittingly or unwittingly allows their account to be used. Criminals often use social engineering techniques to convince victims that they are legitimate payees. As this paper explores below, funds can leave a money mule's account in several ways, for example via transfers to other financial institutions, in cryptocurrency or by cash withdrawals.

In 2023, the Financial Action Task Force (FATF), together with Interpol and the Egmont Group, published a report entitled 'Illicit Financial Flows from Cyber-Enabled Fraud'.[19] The report examines global trends in the laundering of the proceeds of cyber-enabled fraud (CEF), a category of fraud that includes some types of APP fraud.[20] FATF's work clearly demonstrates that these types of fraud have become a transnational form of organised crime: 'The location where CEF predicate offences occur tends to be different from where the ML [money laundering] process occurs. Proceeds can be laundered quickly through a network of accounts, which often span across multiple jurisdictions and financial institutions.'[21] This aligns with the assessment from the National Economic Crime Centre that most fraud in the UK has an overseas component; in 2021, 47% of frauds were estimated

18. UK Finance, 'Annual Fraud Report 2025'.
19. FATF, Interpol and Egmont Group, 'Illicit Financial Flows from Cyber-Enabled Fraud'.
20. The focus of the report is on business email compromise fraud, phishing fraud, impersonation fraud, online trading/trading platform fraud, online romance fraud and online employment fraud. It does not cover other notable types of APP fraud, such as purchase fraud.
21. FATF, Interpol and Egmont Group, 'Illicit Financial Flows from Cyber-Enabled Fraud', p. 3.

to involve offenders from the UK and overseas collaborating, and 30% of frauds estimated to have been conducted by primarily overseas offenders.[22]

The first stage of the laundering is typically the use of a money mule,[23] defined by the UK government as an individual who 'moves the proceeds of crime on behalf of criminals, sometimes in exchange for payment or other benefit'.[24] Money mules have been described as a 'key enabler' of fraud.[25] As set out by the NCA:

> Organised crime groups often use criminal mule networks, with bank accounts owned by witting and unwitting members of the public used to obscure the source and nature of funds. Criminals increasingly use online communication methods to encourage people to become money mules and it is likely that cost of living pressures will continue to attract a wider range of people to such activity.[26]

Money mules can be recruited in a variety of ways, such as fake job advertisements, coercion (for example, some victims of human trafficking may be coerced into becoming money mules) or exploitation (for example, a victim of a romance fraud may be tricked into acting as a money mule).[27] In its evidence to the Home Affairs Select Committee's inquiry into fraud, the FCA highlighted that: 'Fraudsters heavily rely on interconnected mule accounts to transfer and conceal the proceeds of fraud. These transactions can pass through various financial institutions or be converted into cash or cryptocurrencies, effectively masking the money trail, and funnelling the profits back to criminals.'[28]

THE ONWARD MOVEMENT OF FUNDS OUT OF MONEY MULE ACCOUNTS

To better understand the onward movement of funds, Lloyds Bank provided details of transactions worth £7.2 million that left the accounts of known money mules between 17 June 2024 and 11 August 2024. The data consisted

22. Written Evidence Submitted by the National Economic Crime Centre to the House of Lords Fraud Act 2006 and Digital Fraud Committee, 22 April 2022, <https://committees.parliament.uk/writtenevidence/108057/pdf/>, accessed 19 July 2025.
23. FATF, Interpol and Egmont Group, 'Illicit Financial Flows from Cyber-Enabled Fraud'.
24. Home Office, 'Money Mule and Financial Exploitation Action Plan'.
25. *Ibid*.
26. *Ibid.*
27. FATF, Interpol and Egmont Group, 'Illicit Financial Flows from Cyber-Enabled Fraud'.
28. Written evidence submitted by the Financial Conduct Authority (FCA) to the Home Affairs Select Committee on Fraud, 17 April 2024, p. 4, <https://committees.parliament.uk/writtenevidence/129334/pdf/>, accessed 15 May 2025.

of information about the type of payment out, the destination of the payment, the age of the account holder and the account age.

While the focus of this paper is on the transaction flows, it is worth noting that the data from the bank showed that about 20% of known money mule accounts were older than five years, with the majority (about 60%) being older than one year. It appears, therefore, that established accounts are preferred to accounts that have been specifically set up to function as money mule accounts, at least when it comes to traditional banks. Criminal use of longstanding and legitimate accounts can make it harder to spot unusual activity, especially when the proceeds of fraud may be low value and may appear to be in line with the expected activity of the account.

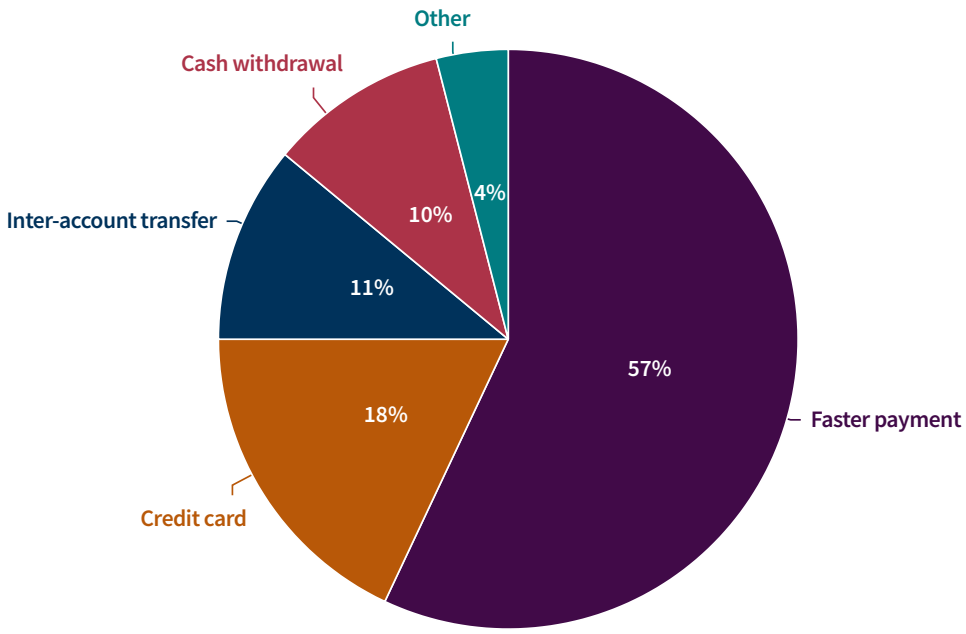
Faster Payments is the main method for the onward transfer of funds. The Faster Payment System was established in the UK in 2008. It allows for real-time payments of up to £1 million between bank accounts in the UK. In 2024, 5.09 billion transactions valued at £4.2 trillion were sent via Faster Payments.[29] While the overwhelming majority of Faster Payments are entirely legitimate, the ability for criminals to transfer money between accounts almost instantaneously is often cited as a reason for the growth in APP fraud.[30] The data collated by UK Finance shows that Faster Payments were used for 96% of APP fraud cases in 2024.[31] By the time a victim realises that they have become a victim of fraud and reported it to their bank, the funds may have already moved through multiple accounts, thus becoming almost impossible to trace quickly enough to recover any funds.

Faster Payments continue to be a popular route for the onward movement of cash from a money mule's account

The data from the bank shows that Faster Payments continue to be a popular route for the onward movement of cash from a money mule's account – making up 57% of outbound payments. Of the value of payments received into the money mules' accounts in the sample, nearly 28% left the account within 15 minutes and a further 25% left within an hour. Less than 15% of the money remained within the accounts after 24 hours. This demonstrates the clear preference for moving money quickly onwards from a mule's account. It is notable, however, that Faster Payments do not dominate payments out of mule accounts in the same way that they dominate payments into accounts – there are many ways, in addition to Faster Payments, that money can be moved onwards.[32] For example, nearly one-fifth of payments out of a money mule's account are via debit card spending, and one tenth of the money is cashed out via withdrawals at ATMs or bank branches.

29. Pay.UK, 'Faster Payment System', <https://www.wearepay.uk/what-we-do/payment-systems/faster-payment-system/>, accessed 15 May 2025.
30. House of Lords Fraud Act 2006 and Digital Fraud Committee, 'Fighting Fraud: Breaking the Chain', HL Paper 87, Report of Session 2022–23, paras 214–15.
31. UK Finance, 'Annual Fraud Report 2025'.
32. See also Jo Braithwaite, '"Authorized Push Payment" Bank Fraud: What Does an Effective Regulatory Response Look Like?', *Journal of Financial Regulation* (Vol. 10, No. 2, 2024), pp. 174–93.

Figure 1: Share of Payments Out of Money Mule Accounts, by Type



Source: Data provided by Lloyds Bank.

TYPES OF PAYMENTS OUT OF MONEY MULE ACCOUNTS

TRANSFERS VIA THE FASTER PAYMENT SYSTEM

As noted above, 57% of funds in money mule accounts leave via the Faster Payment System. In the period covered by the data, this amounted to 7,631 transactions valued at £4.06 million with an average payment amount of £532. Of these, 38% of the payments by total value went to just three banks/payment firms, with 20% of all payments by total value going to one single firm. This firm also received the highest number of payments from money mule accounts. These three institutions can be characterised as digital financial institutions, offering banking and money transfer services via apps and online banking.

Data published by the PSR – which started publishing annual performance data on APP fraud in 2023 – also demonstrates the use of smaller online banks and payment firms in the laundering process.[33] Metric C of the PSR's data relates to the value and volume of APP frauds received into the bank/firm's account. The data covers the 14 largest banking groups in the UK.

33. PSR, 'APP Fraud Performance Data', <https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/>, accessed 15 May 2025.

These banks, known as 'directed payment service providers (PSPs)',[34] are required to submit data to the PSR. The 'non-directed PSPs' are smaller firms that are identified as one of the top 20 receivers of the proceeds of APP fraud by value and/or volume, based on the data submitted by the directed PSPs.

The PSR's data shows a significant difference in the payment patterns of directed and non-directed PSPs. The non-directed PSPs receive a disproportionately large share of payments related to fraud compared with the overall share of transactions that they receive. The PSR's analysis shows that non-directed PSPs accounted for just over 8% of all Faster Payments made in 2023, but received 53% of all fraudulent transactions.[35] The seeming preference that some criminals have for using smaller financial institutions to launder the proceeds of APP fraud is also highlighted by the FATF in its 2023 report. This states that:

> The evolution of financial payments has resulted in new digital financial institutions, such as payment service providers (PSPs), the issuance of e-money etc. Traditional FIs [financial institutions] may have more resources at their disposal, which may result in relatively more robust controls compared to these newer digital financial institutions. This may lead to displacement, where criminals seek to exploit vulnerabilities in these alternative financial providers to launder funds.[36]

The author interviews – conducted as part of the research for this paper – with a number of experts validated this finding. They expressed the view that some of the smaller firms had less robust financial crime controls, particularly for customer onboarding, and criminals were able to exploit these weaknesses.[37] Several interviewees felt that the onboarding controls of digital financial institutions were relatively weak due to the focus that many of these firms have on customer acquisition and growth, and that compliance programmes are not able to keep up. The FCA's 2022 review of challenger banks expressed a similar view,[38] and this has been reflected in subsequent enforcement action taken by the regulator.[39]

---

34. Directed PSPs are those PSPs in scope of the Payment Systems Regulator's (PSR) Specific Direction 20 (SD20). They are required to provide the PSR with performance data on APP fraud.
35. PSR, 'Faster Payments APP Scams: Changing the Maximum Level of Reimbursement', CP24/11, September 2024, <https://www.psr.org.uk/media/pvwjsf2n/cp24-11-faster-payments-max-reimbursement-sept-2024.pdf>, accessed 15 May 2025.
36. FATF, Interpol and Egmont Group, 'Illicit Financial Flows from Cyber-Enabled Fraud', p. 27.
37. Author interview with financial services professional, online, August 2024; author interview with fraud expert, online, August 2024; author interview with representative from law enforcement, online, October 2024.
38. FCA, 'FCA Review Finds Weaknesses in Some Challenger Banks' Financial Crime Controls', 22 April 2022, <https://www.fca.org.uk/news/press-releases/review-weaknesses-challenger-banks-financial-crime-controls>, accessed 15 May 2025.
39. FCA, 'FCA Fines Starling Bank £29m for Failings in their Financial Crime Systems and Controls', 2 October 2024, <https://www.fca.org.uk/news/press-releases/

The data from Lloyds Bank also demonstrates how criminals can use new types of financial products, such as banking-as-a-service (BaaS) products, as part of the laundering process. BaaS providers give other companies, such as startup FinTechs, access to their banking infrastructure. This access allows them to use the BaaS provider's banking licence to provide banking services, such as payment processing or lending, to their customers. This is sometimes known as 'white labelling': the end customer is presented with a user interface that is branded as the startup, although the underlying functionality is provided by a third party, the BaaS provider. As a result, a BaaS provider is one step removed from the underlying customer, and this has raised concerns over the risk of BaaS products facilitating financial crime.[40]

The FATF report on money laundering from CRF also identified the risks associated with these types of products. It states that:

> The payments network can also be fragmented. There can be various nested financial relationships between these institutions, e.g., with various payments institutions transacting with one another or providing accounts to smaller providers, who in turn provide other types of financial services … This fragmentation can also intensify the difficulties in tracing transactions across various types of institutions in the "payment chain". This may also pose challenges in ensuring the immediate availability of basic information on the originator and beneficiary of transfers across the payment chain.[41]

The data provided by Lloyds Bank shows that over 450 (10%) of the payments identified from mule accounts went to these BaaS providers – a disproportionate share compared with the overall share of Faster Payments to these services.[42] This finding is echoed by the data published by the PSR. This data includes three BaaS providers within the list of worst-performing firms, by volume of fraud-linked payments received per million transactions in 2023 (although it should be noted that several services have improved on their performance from the prior year).[43]

PAYMENTS VIA DEBIT CARDS

Traditionally, criminals have looked to use the Faster Payment System to move money out of an account as soon as possible. However, the data from Lloyds Bank – validated by discussions held with relevant experts – suggests that there is greater diversification in the methods for moving money onwards,

---

fca-fines-starling-bank-failings-financial-crime-systems-and-controls>, accessed 15 May 2025.

40. Koos Couvée, 'EU, US Regulators Take Long Look at "Banking-as-a-Service" Platforms', *moneylaundering.com*, 21 April 2023, <https://www.moneylaundering.com/news/eu-us-regulators-take-long-look-at-banking-as-a-service-platforms/>, accessed 15 May 2025.
41. FATF, Interpol and Egmont Group, 'Illicit Financial Flows from Cyber-Enabled Fraud'.
42. This statistic was confirmed by the bank.
43. PSR, 'APP Fraud Performance Data'.

as banks and payment firms have looked to strengthen their controls for inbound payments. Debit card spending is an increasingly popular method of moving the proceeds of fraud. Experts further noted that they expect this to increase, particularly as the new customer reimbursement requirements introduced in the UK in 2024 require firms to strengthen controls over bank transfers even further.[44]

The amount of money leaving mules' accounts via debit card purchases may also show that a proportion of the proceeds of crime are lost along the way and are used for everyday living expenses, rather than being laundered in the traditional sense. This mirrors academic findings on other types of revenue-generating crime.[45] While the academic research is generally based on money laundering associated with drugs, the evidence from the data suggests that this is also true for fraud, at least in terms of money mule activity. While a fraud may have cost a victim £1,000, a lesser amount may end up in the hands of the criminal who perpetrated the fraud once, for example, fees are paid to the money mule for the use of their account.

The data from Lloyds Bank shows that there were 12,336 transactions on debit cards from money mules' accounts in the two-month period covered, totalling £1.33 million. The average value of each payment was £107. While a very large number of the payments appear to be for general expenses – such as food, drink and taxis – or for one-off large amounts to a particular retailer of high-value goods, it is also noticeable that the debit card payments include significant volumes to money transfer services, foreign exchange companies and crypto exchanges.

By value, the top recipient of debit card payments is a global remittance business that allows users to make cross-border payments. Based on the company's website, the top destinations for UK users to send funds to are India, Pakistan and the Philippines. Other similar businesses feature in the top 10 destinations. In some cases, the average payments to these companies are relatively small. However, there is a high volume of transactions. The third most popular outlet for debit card purchases is a crypto exchange, with a foreign exchange business placed fifth.[46] While there are legitimate use cases for all of these types of service – for example, sending money to family members in other countries – the prevalence of these types of firms in the debit card data indicates that they may be forming part of the onward money laundering and could indicate one of the ways in which in which the funds are transferred onwards overseas and/or into cash or cryptocurrencies.

44. Discussions with representatives from Lloyds Bank.
45. See, for example, Mike Levi and Melvin Soudijn, 'Understanding the Laundering of Organized Crime Money', *Crime and Justice* (Vol. 49, 2020), pp. 579–632.
46. The destination in fourth place is a company to which four large payments were made in the period. It is not possible to determine exactly the recipient, although the name in the data matches a telecommunications company based in an overseas jurisdiction.

CASH

The data provided by Lloyds Bank shows that 10% of the funds from known money mule accounts are withdrawn directly as cash either at an ATM or within a branch. As noted above, the data from debit card purchases also includes examples of money being converted into cash, for example at foreign exchange bureaus.

Cash still remains a popular vehicle for moving the funds from organised crime, including fraud. It can break the connection between a crime that generated profits electronically – which may be traceable across the financial system – and the criminal proceeds, thus allowing criminals to better evade detection.[47] The FATF's report on CEF provides examples of fraud cases from around the world. It details cases of withdrawals of cash at ATMs by mules or by members of the criminal network. The physical cash may then be moved cross-border and deposited in a bank in a different jurisdiction, as well as being used to fund a criminal lifestyle.[48]

Cash ... can break the connection between a crime that generated profits electronically and the criminal proceeds

CRYPTOCURRENCIES

The convergence of fraud and cryptocurrency has seen fraud schemes evolving at pace. Concern around the convergence of fraud and cryptocurrency has been reflected in government reports, with the FBI noting an increased number of complaints referencing cryptocurrency in 2024.[49] APP frauds may result in the victim themselves transferring funds into cryptocurrencies, as happens in some types of investment fraud or romance fraud,[50] or the proceeds from an APP fraud may be transferred via cryptocurrencies at some point in the laundering process.

There is no clear evidence in the dataset on the volume or value of APP frauds that are ultimately transferred via cryptocurrencies at some point. However, the transaction data from the bank shows some initial purchases made by money mules with debit cards. Within the dataset, 94 debit card transactions, valued at £54,049, were made at large, centralised cryptocurrency exchanges. In addition, one service provider that identifies itself as a decentralised cryptocurrency on and off ramp is associated with 17 transactions involving the use of a debit card, which equates to £4,501. Given the scale of the global cryptocurrency market, it is not surprising that

47. Rian Matanky-Becker, 'High-End and Cash-Based Money Laundering: Defining and Disaggregating Complex Phenomena', *European Journal on Criminal Policy and Research* (Vol. 30, 2024), pp. 421–33.
48. FATF, Interpol and Egmont Group, 'Illicit Financial Flows from Cyber-Enabled Fraud'.
49. Internet Crime Complaint Center, 'Federal Bureau of Investigation Internet Crime Report 2024', <https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf>, accessed 24 June 2025.
50. Daniel Holmes, 'Unpicking the Anatomy of a Crypto Scam', UK Finance, <https://www.ukfinance.org.uk/news-and-insight/blogs/unpicking-anatomy-crypto-scam>, accessed 15 May 2025.

there is evidence of the purchase of cryptocurrencies in the dataset, albeit at a limited scale. However, one interviewee for this paper confirmed that they had seen similar patterns of transactions at other financial institutions, with suspected criminal funds being used to purchase cryptocurrencies with a debit or credit card at a third-party exchange.[51] As with the use of debit cards, this demonstrates the importance of acknowledging the diversity of methods for laundering money through the financial system, beyond the use of Faster Payments.

FOLLOWING THE FRAUD

The data analysed for this paper shows the next step in the chain once a money mule has received the proceeds of a fraud. Piecing together the flow associated with a single fraud is likely to be an almost impossible task, given the speed at which payments move and the ability for criminals to transfer the proceeds in and out of different stores of value, such as cash, cryptocurrencies or high-value assets. It is also the case that a significant proportion of frauds – estimated at somewhere between one-quarter and one-third – result in losses of less than £100.[52] Therefore, considering fraud losses at an aggregate level and how the consolidated amounts are laundered is more instructive than following the flow of funds of an individual fraud.

As set out earlier, some of the proceeds of fraud are lost along the way in what can be best described as business expenses. This may include not only fees to money mules, but also the purchase of criminal goods and/or services, for example on online marketplaces. An example of an online marketplace was a platform called Russian Comms, which was shut down by the NCA in 2024. Russian Comms allowed users to spoof phone numbers, thus tricking potential victims into thinking that the caller was calling from a legitimate telephone number. Access to the full service was charged at £350 per month, to be paid via cryptocurrency.[53] Similarly, Genesis Market, described as 'one of the most dangerous [criminal] marketplaces', sold personal data and account credentials stolen from over 1.5 million computers worldwide and received millions of dollars of payments in cryptocurrencies.[54]

51. Author interview with representative of a technology provider, online, August 2024.
52. *FinTech Times, '*Only 4 in 21 Major Banks Agree to Cover First £100 of Any APP Case as PSR Rule Comes into Effect', 9 October 2024, <https://thefintechtimes.com/only-4-in-21-major-banks-agree-to-cover-first-100-of-any-app-case-as-psr-rule-comes-into-effect/>, accessed 15 May 2025.
53. *BBC News,* 'Fake Caller App Shut after Thieves Duped Thousands', 2 August 2024.
54. TRM, 'Genesis Market: Understanding Law Enforcement's Recent Actions', 26 July 2023, <https://www.trmlabs.com/post/genesis-market-understanding-law-enforcements-recent-actions>, accessed 15 May 2025.

Box 1: The Impact of Fraud on the Vulnerable: The Black Axe Group and the KK Park Scam

Fraud and the associated money laundering can have a devasting impact on some of the most vulnerable people in the world. Two examples, the Black Axe group in Nigeria and the KK Park scam compound in Myanmar, demonstrate just how closely intertwined fraud is with other forms of transnational organised crime.

The Black Axe group, originating in Nigeria, is engaged in a large number of serious crimes including drug trafficking, smuggling, kidnapping, prostitution and violence. However, its most profitable activity by far is online fraud, and the group is thought to have made tens of billions of dollars from victims all over the world, including many in the UK.[55] A complex network of international money launderers transfers the victims' funds around the world, purchasing luxury cars and real estate, and using the funds to fund the group's other criminal activities. The money that the Black Axe group makes fuels political instability within Nigeria, and the group preys on vulnerable young men who are forced to join the gang with the promise of a steady income and are then unable to escape a life of crime.[56]

The KK Park scam compound in Myanmar is one of the most notorious scam compounds in Southeast Asia.[57] At one stage, it was estimated that there were over 2,000 workers there, most of whom had been trafficked against their will.[58] Their job is to make contact online with potential fraud victims. Workers in these kinds of compounds are held as slaves, beaten, tortured and starved if they do not meet their targets.[59] It has been shown that cryptocurrency wallets associated with KK Park have received millions of dollars of cryptocurrencies, primarily the proceeds of romance scams. The same wallets have also been shown to have received ransom payments in cryptocurrencies from family members of those enslaved workers who are being forced to work in the compounds.

55. Matthew La Lime, 'Black Axe—Nigeria's Most Notorious Transnational Criminal Organization', Africa Center for Strategic Studies, 29 October 2024, <https://africacenter.org/spotlight/black-axe-nigeria-transnational-organized-crime/>, accessed 15 May 2015.
56. *BBC News,* 'World's Police in Technological Arms Race with Nigerian Mafia', 28 August 2024.
57. Chainalysis, 'The On-Chain Footprint of Southeast Asia's "Pig Butchering" Compounds: Human Trafficking, Ransoms, and Hundreds of Millions Scammed', 24 February 2024, <https://www.chainalysis.com/blog/pig-butchering-human-trafficking/>, accessed 15 May 2025.
58. *Ibid.*
59. *Ibid.*

CONCLUSION: INFORMING THE POLICY RESPONSE TO FRAUD

In May 2023, the Home Office published the UK's Fraud Strategy, subtitled 'Stopping Scams and Protecting the Public' and aimed at cutting fraud by 10%.[60] The strategy was formed on three pillars: pursuing fraudsters; blocking fraudsters; and empowering the public.[61] To date, most of the efforts – both of industry and law enforcement – have been directed towards stopping fraud at the source and disrupting criminal activity before it has happened. This is critical and should remain a priority for policymakers, regulators, law enforcement and industry, not least because of the significant emotional damage caused to victims of fraud. However, ultimately, organised crime is about making money. If interventions, whether from law enforcement or the industry, can make it harder for criminals to realise the profits from their crimes, it removes some of the incentives for criminals to commit fraud in the first place.

To do this, this paper identifies four key considerations for policymakers, regulators, law enforcement and industry.

The system is only as strong as the weakest link

1. **The system is only as strong as the weakest link**. Small payment firms and digital banks have come under scrutiny in recent years. Data from the PSR shows that such firms facilitate a disproportionate amount of fraudulent transactions compared with their overall market share. The evidence from this paper suggests that poor controls at smaller institutions continue to undermine the UK's ability to prevent and disrupt fraud. New entrants to the market, such as BaaS providers, also appear to be being exploited by fraudsters. This calls for a robust regulatory response.
2. **Beware the displacement risk**. The data analysed for this paper shows that nearly 20% of the funds received by money mules exit the accounts via debit card activity. This is likely to continue to rise as more banks and payment firms must strengthen their customer onboarding controls and inbound transaction monitoring controls in response to regulatory scrutiny. Debit card usage may also increase as banks and payment firms are allowed extra time to hold payments to investigate potentially suspicious transactions, thus requiring criminals to seek alternative exit routes. Displacement leading to diversification will make it harder to identify the criminals who profit from fraud. Further research is needed to understand how this activity is changing and to manage the displacement risk.
3. **Data-sharing at the level of transactions can be powerful**. The data in this paper was provided by one bank. If it were combined with data for the same period from multiple other financial institutions – including cryptocurrency exchanges – it would likely provide a

60. HM Government, *Fraud Strategy.*
61. At the time of writing, the UK government was engaged in developing a new and expanded fraud strategy.

richer insight into the onward transfer of funds. Data-sharing has the potential to revolutionise the fight against fraud, and efforts such as the public–private partnership, launched by the NCA and seven UK banks, are to be commended.[62] However, to derive the most benefit, such partnerships need to involve a larger number of financial institutions, including smaller banks and payment firms, BaaS providers and cryptocurrency service providers.

4. **Speed is of the essence**. The evidence for this paper shows that over half of the funds received by known money mules left their accounts within an hour; of these transfers, over half took place in less than 15 minutes. This demonstrates the crucial importance of moving towards a model of real-time, or close to, data-sharing across the entire system, allowing both the private sector and law enforcement to react at speed when a fraud is identified.

ABOUT THE AUTHORS

Kathryn Westmore is a Senior Research Fellow at RUSI's Centre for Finance and Security. She leads the Financial Crime Policy Programme which tracks the development and implementation of effective anti-financial crime policies, regulations and standards.

Allison Owen is an Associate Fellow at RUSI's Centre for Finance and Security. Her primary research projects focus on the policy and security dimensions of cryptocurrency and new payment methods. She supports RUSI by researching emerging financial crime threats and delivering training on the material for the private and public sectors.

62. NCA, 'Ground Breaking Public Private Partnership Launched to Identify Criminality Using Banking Data', 26 July 2024, <https://www.nationalcrimeagency.gov.uk/news/ground-breaking-public-private-partnership-launched-to-identify-criminality-using-banking-data>, accessed 15 May 2025.