www.rusi.org

RUSI

Conference Report

Who Do You Think You Are?

Recommendations on the Future Response to Large-Scale Identity Fraud

Conference Report

193 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 193 years.

RUSI Conference Report, November 2024.

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)

Who Do You Think You Are? Recommendations on the Future Response to Large-Scale Identity Fraud

Introduction

Fraud has reached 'epidemic' levels globally[1] and is the most commonly experienced crime in the UK, reaching an unprecedented 40% of all crime in the UK in 2022.[2] The growing and rapidly evolving fraud threat is increasingly being recognised as a threat to the UK's economic security and, by extension, its national security.[3]

Within the broader fraud threat, identity fraud is a growing area of concern. Identity fraud occurs when an individual's personal details are stolen or compromised (known as identity theft) and used to facilitate a crime, usually for financial gain, but also sometimes to facilitate crimes requiring the obfuscation of identity, such a money laundering, terrorism or immigration crime.

Identity fraud for financial gain (hereafter referred to as identity fraud) is estimated to cost the UK economy £1.8 billion per annum.[4] It represents the largest category of cases filed to the National Fraud Database (a cross-industry, counter-fraud data-sharing solution administered by the not-for-profit organisation

1. Interpol, 'INTERPOL Financial Fraud Assessment: A Global Threat Boosted by Technology', 11 March 2024, <https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology>, accessed 5 November 2024.
2. HM Government, *Fraud Strategy: Stopping Scams and Protecting the Public* CP 839 (London: The Stationery Office, 2023), <https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf>, accessed 5 November 2024.
3. UK Finance, 'UK Finance Calls for Urgent Action from all Sectors as Fraud Continues to Threaten the UK', 13 October 2022, <https://www.ukfinance.org.uk/news-and-insight/press-release/uk-finance-calls-urgent-action-all-sectors-fraud-continues-threaten>, accessed 5 November 2024.
4. Tim Robinson et al., 'Annual Fraud Indicator 2023', Crowe, Peters & Peters and the University of Portsmouth, 2023, p. 20, <https://www.crowe.com/uk/insights/annual-fraud-indicator>, accessed 20 November 2024.

Cifas), accounting for over two-thirds of all industry case filings in 2023, or 237,642 individual cases.[5]

While the importance of building a robust response to identity fraud in the UK is recognised in the previous government's Fraud Strategy, more must be done to tackle the threat.[6] In response to growing concerns in industry about the scale of identity fraud and to help inform the UK government's future fraud strategy, in October 2024, RUSI's Centre for Finance and Security and Cifas hosted a roundtable to discuss how to tackle identity fraud. Participants were drawn from financial institutions, regulatory technology companies, credit rating agencies and policymaking roles.

The roundtable focused on articulating the current nature of the threat and identifying a range of policy, legislative, operational and technical interventions to inform the next UK fraud strategy. Discussions focused on responses to identity fraud for financial gain rather than other types of criminal behaviour, although participants also recognised the need to examine overlapping enablers. The roundtable looked first at the evolution of identity fraud and how identity theft and identity fraud are treated under UK law. It then considered the current approach to identity fraud in the UK to examine what was working well and what could be augmented. Finally, it examined the gaps in the UK's response to identity fraud, and identified a series of recommendations.

The discussions were held on a non-attributable basis and this conference report sets out the main themes of the conversation without identifying comments made by any specific participants. While the roundtable participants drew on their experience on identity fraud in the UK, it was recognised that identity fraud is an enabler of transnational organised crime and hostile state activity, and therefore it is hoped that the recommendations from the roundtable will be of benefit to stakeholders beyond the UK.

The Evolution of Identity Fraud

One participant used the metaphor of the frog being slowly boiled over time to explain how the threat of identity fraud has been allowed to grow unchecked over the past decade. Enabled by growing digital connectivity and increased remote onboarding in the financial sector, identity fraud, participants noted, had now reached a scale where it had the potential to stymie economic growth and investment in the financial sector, as well as have a significant impact on victims and consumers.

5. Cifas, 'Fraudscape 2024', <https://www.fraudscape.co.uk/#identity-fraud>, accessed 13 November 2024.
6. HM Government, *Fraud Strategy*, p. 4.

Participants discussed the ways in which identity fraud had changed significantly in the digital age. Whereas identity fraud traditionally has relied on the use of physical documents and/or so-called 'document factories',[7] the rise of the provision of online services means that physical identity documents are no longer necessary to commit most identity fraud; for example, many financial institutions allow customers to open an account via an app with an image of an identity document.

Mainly facilitated by large-scale data leaks and systematic phishing,[8] the act of gaining access to key identity details online is the essential 'seed crime' for the mass-scale identity fraud of today. Largely operating as a 'crime as a service', these data leaks were traditionally sold on the dark web, but increasingly can be found advertised on the surface web on social media channels and in closed communication networks.[9]

As regards consumer protection, all participants agreed that the scale of data hacks and leaks means that approaches which focus solely on encouraging consumers to protect their own data are increasingly redundant. Essentially, we should all assume our data is out there and at risk. Interventions to limit the use of compromised data were therefore seen by participants as the priority.

At an industry level, there was unanimous agreement that the problem was on the cusp of acceleration, given the easier access for criminals to AI and deep-fake technologies that facilitate high-quality document manipulation.[10] While the current counter-fraud technologies employed by larger institutions pick up most of these fakes, the industry is in an arms race; over time, the use of AI will improve, making fake documentation harder to spot, and the industry may struggle to keep up. Participants had already seen evidence of criminals evading onboarding controls using AI-generated identity documents.

However, despite pockets of knowledge regarding the scale, nature and impact of the identity fraud threat, it was widely agreed that the lack of a comprehensive common understanding across the public and private sectors on how the threat had changed over time was hampering the response. There are particular knowledge gaps on the ways in which the criminal facilitation of access to identity

7. Document factories are criminal enterprises involved in the production of fake or fraudulently obtained identity documentation.
8. Phishing is the practice of sending emails or other messages with the aim of inducing individuals to reveal personal information.
9. Warwick Ashford, 'Surface Web Used in Private Data Sales', *ComputerWeekly.com*, 19 June 2018, <https://www.computerweekly.com/news/252443314/Surface-web-used-in-private-data-sales>, accessed 21 November 2024.
10. This problem has since been articulated in an advisory note from the US financial intelligence unit, FinCEN. See FinCEN, 'FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, 13 November 2024, <https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial>, accessed 21 November 2024.

data for financial fraud intersects with the 'market' for those seeking to use identity fraud for identity obfuscation purposes, such as to facilitate serious organised crime, terrorism and sanctions evasion.

It was felt that the first principle of tackling identity fraud should be to update collective understanding of the prevailing typologies and the intersection of identity theft and fraud, to ensure that future interventions across the public, private and third sectors adequately respond to this threat.

Recommendation 1: The UK government should commission further research into the changing nature of the identity fraud threat and its societal and economic impact, as well as its intersection with other national security threats, including transnational organised crime and hostile state activity.

Identity Theft and Identity Fraud in UK Law

Under UK law, the theft or purchase of identity details is not a recordable offence; it only becomes a criminal offence when those identity details are used for the purposes of committing a crime.[11] In a 2022 report, the House of Lords Fraud Act 2006 and Digital Fraud Committee recommended that the government consult on the introduction of legislation to make identity theft itself a criminal offence.[12]

Most participants felt that police recording of cases of identity theft is extremely limited, partly due to the lack of a criminal offence. This contributes to the lack of understanding on the scale of the threat in the UK. It was also felt that the lack of a specific offence had led to a downgrading of the importance of the issue of identity theft within policing, despite the role of identity theft in enabling a wide range of criminality, including identity fraud.

However, participants in the roundtable were divided as to the merits of introducing a specific criminal offence of identity theft, given that, from a practical perspective, activities which constitute identity theft can be prosecuted under existing legislation, including the Computer Misuse Act 1990, the Identity Documents Act 2010 and the Fraud Act 2006. In short, most participants felt that the issue lay more in the application of the law than in the law itself. However,

11. The Fraud Act 2006 contains an offence of fraud by false representation. See Fraud Act 2006, section 2, <https://www.legislation.gov.uk/ukpga/2006/35/section/2>, accessed 20 November 2024.
12. The report noted: 'Identity theft is a fundamental component of fraud and is routinely used by fraudsters to steal money from legitimate individuals and organisations yet it remains out of scope of criminal offences'. See House of Lords Fraud Act 2006 and Digital Fraud Committee, 'Fighting Fraud: Breaking the Chain', Report of Session 2022–23, 12 November 2022, paras 458–59, <https://committees.parliament.uk/publications/31584/documents/177260/default/>, accessed 20 November 2024.

others thought that there would be a stronger deterrent effect if law enforcement had the ability to bring charges specifically for identity theft in a simple and consistent way.

The debate demonstrated that there is no simple response to the question of whether identity theft should be criminalised or not and that more work needs to be undertaken to understand the benefit of a specific offence and any unintended consequences.

Recommendation 2: The UK government's planned review of fraud legislation should consider the pros and cons of expressly criminalising acts that contribute to identity theft.

The Current Response to Identity Fraud – Scaling Up

Having established the changing nature of the threat of identity fraud and its status under UK law, participants discussed aspects of the current response and how these could be improved.

The Operational Response

At an operational policing level, participants agreed that to date, identity fraud had been under-prioritised. Identity theft acts as an enabler to all manner of criminal activities, but participants felt law enforcement professionals were sometimes more reticent to investigate identity theft – whether due to unwillingness, lack of knowledge, or both – than they were to investigate the crime that was committed with the stolen identities. The lack of a clear legal framework for identity theft, as set out in the previous section, was also considered by participants to be a contributing factor.

However, participants also recognised that the scale of the threat far outstripped policing resources to deal with identity theft on a case-by-case basis. Participants broadly praised the recent focus of law enforcement on disruptive activities, such as taking down key criminal online marketplaces, rather than dealing with individual offenders further down the 'value chain'.[13] It was agreed that tackling the enabling criminal architecture and those individuals key to the sale of identity details was the best use of limited resources.

13. For example, Metropolitan Police, 'Operation Elaborate', April 2023, <https://www.met.police.uk/elaborate>, accessed 13 November 2024.

Recommendation 3: Law enforcement should continue to focus operational activity on identity theft markets and key identity data-brokering intermediaries. This also includes identifying both the displacement impact of successful law enforcement operations and to where criminals might turn instead to access the data they need to commit identity fraud.

Public–Private Data Sharing

Participants noted previous good practice in public–private data sharing to tackle identity fraud through the sharing of false or 'fraudulently obtained genuine' (FOG) identity document data, under Operation Amberhill.[14] This operation is an initiative led by the Metropolitan Police Service, whereby a central team collates and distributes data on false and FOG identities and shares it with public and private sector partners. Participants agreed that the sharing of this data had a considerable impact, preventing millions of pounds of losses to industry every year.

However, participants believed that funding for this service has significant reduced over time. Participants strongly agreed that the refunding and restoring of this essential function should be an immediate priority, and that this service should be modernised to include by both physical and digital false and FOG identity data collation and application programming interface (API) connectivity.[15]

Recommendation 4: Revitalise Operation Amberhill, with additional resources and funding, including to expand its remit to include digital false and FOG identity documentation.

Consumer Protection

Participants identified a range of successful industry-led initiatives underway to enable consumers to protect themselves following the theft of their identity. This includes 'credit score locking'[16] via credit reference agencies and the use of protective registration services[17] to alert the credit industry to potential identity misuse. Participants noted the importance of these initiatives to consumers, but also that consumers have to pay a fee for these kinds of services and that they generally only access the services after an incident has occurred. It was

14. Cabinet Office, 'National Fraud Initiative', 4 November 2016, p. 32, <https://assets.publishing.service.gov.uk/media/5b8fa6d9ed915d1ee3326f8d/nfi_national_report_2016.pdf>, accessed 20 November 2024.
15. An API is a software interface between two different programmes.
16. See, for example, Experian, 'Experian CreditLock', <https://www.experian.com/protection/creditlock/>, accessed 13 November 2024; Equifax, 'Credit Lock Alert, <https://www.equifax.com/personal/products/credit/credit-lock-alert/>, accessed 21 November 2024.
17. Cifas, 'I Want to Apply for Protective Registration', <https://www.cifas.org.uk/pr>, accessed 13 November 2024.

agreed that the use of more preventive technologies and increased proactive alerts when consumers are applying for credit would reduce identity fraud. However, it was unclear how much 'friction' consumers would be willing to tolerate in the process, and participants felt that more research was needed to explore this.

Recommendation 5: The financial industry should conduct consumer attitudes surveys to explore consumer tolerance for increased 'friction' in the consumer credit application process, designed to reduce the threat of identity fraud.

Digital Identity

The UK government has put in place legislation to increase trust and confidence in digital identity[18] through the introduction of the Data (Use and Access) Bill 2024,[19] which will implement a digital verification services 'trust framework'.[20] Participants generally viewed digital identity as a positive initiative that is likely to play a part in reducing identity fraud. However, participants felt that there were two key factors likely to limit the role of digital identity in reducing identity fraud over the medium term.

First, it was widely agreed that uptake of digital identity by UK consumers was slow when compared to other countries. This is likely due to the lack of a 'culture' of national identity verification, given the UK's lack of a physical identity card scheme.

Second, some participants noted the variable levels of counter-fraud standards across the identity verification industry and that, given that the trust framework is non-compulsory, the variability in standards may lead to digital identities becoming a new vector of the identity fraud threat. Ensuring that the new Office for Digital Identities and Attributes[21] actively reviews the counter-fraud standards of companies operating under the trust framework and reviews the standards annually is key to preventing this.

18. A digital identity is a digital representation of an individual's identity information used to verify aspects of their identity in the digital economy. The UK, unlike European counterparts, does not have a centralised digital identity programme, and under the Digital Use and Access Bill 2024, is establishing a commercial-led system governed through a 'trust mark'. See Hannah Rutter, 'A Way to Prove Who You Are That is Fit for the UK's Digital Economy', Office for Digital Identities and Attributes, 24 October 2024, <https://enablingdigitalidentity.blog.gov.uk/2024/10/24/a-way-to-prove-who-you-are-that-is-fit-for-the-uks-digital-economy/>, accessed 21 November 2024.
19. UK Parliament, 'Data (Use and Access) Bill', 23 October 2024, <https://bills.parliament.uk/bills/3825>, accessed 13 November 2024.
20. HM Government, 'Enabling the Use of Digital Identities in the UK', 1 November 2024, <https://www.gov.uk/guidance/digital-identity#standards-for-digital-identities-and-attributes>, accessed 21 November 2024.
21. The Office for Digital Identities and Attributes, 'About Us', <https://www.gov.uk/government/organisations/office-for-digital-identities-and-attributes/about>, accessed 29 November 2024.

Recommendation 6: Ensure that counter-fraud measures within the digital verification services trust framework are kept fit for purpose through robust annual review.

Response Gaps – Priority Areas for the Future Fraud Strategy

The roundtable went on to discuss some of the key gaps in the response to the identity fraud threat, to inform areas to which the UK government's future fraud strategy could contribute. Particular gaps were highlighted in relation to victim support and the sharing of public sector data with industry.

Support for Victims

It was widely agreed that victims of identity fraud were poorly served by policing and wider government agencies. This is particularly the case where the victim has not personally suffered a financial loss; anecdotally, some participants reported that victims were told by the police that they were not actually 'victims' given the financial institution more often than not suffered the financial loss.[22]

Participants agreed strongly that the current narrative underplayed wider psychological impacts on individuals who may feel threatened by the theft of their identity as well as affected by the significant administrative burden and potential damage to their credit scores. The fact that identity fraud is often unearthed when the consumer applies for legitimate credit, such as a mortgage, which is subsequently refused, is another way in which identity fraud can have a significant impact on the victim, despite the fact that the fraud itself may have caused no direct loss to them.

While recent initiatives, such as the launch of the Home Office's Identity Theft checklist, were welcome, participants agreed that more needed to be done to improve understanding of the impact of identity theft and fraud on victims.[23] Participants pointed to the victim support services provided by the industry[24]

22. A high proportion of cases of identity fraud for financial gain take the form of fraudulent applications for credit in the victim's name. Once the victim has proven that they did not make the application themselves, they are no longer legally obliged to repay the credit, meaning that the financial institution bears the financial loss.
23. Home Office, 'Identity Theft Victims' Checklist', <https://data.actionfraud.police.uk/cms/wp-content/uploads/2023/12/Identity-theft-victims-checklist.pdf>, accessed 5 November 2024.
24. For example, see Experian, 'What to Do if You're a Victim of Identity Fraud', <https://www.experian.co.uk/consumer/identity/what-to-do-if-victim.html>, accessed 21 November 2024.

and the third sector[25] in the UK, and felt that it would be beneficial for the UK government to endorse these schemes, as in Australia and New Zealand.[26]

Recommendation 7: The UK government's next fraud strategy should consider further work to understand the impact, beyond financial losses, on victims, and the government should work with the industry and third sector to establish government-endorsed sources of support for victims.

Enhanced Data Sharing

While Operation Amberhill was highlighted as an example of good practice – albeit one that now requires further investment – participants felt that more could be done by the public sector to provide industry with greater access to information and intelligence to improve its ability to act as the first line of defence in the UK against identity fraud.

First, participants felt that there was a lack of data sharing by police with established industry data-sharing schemes, such as the National Fraud Database. While recognising the challenges of sharing data in relation to sensitive law enforcement operations and in compliance with data-protection principles, participants raised the potential for sharing non-identity-related attributes, such as device and IP data associated with the commission of identity-related crimes.

Second, industry participants highlighted the importance of near real-time data sharing between the public and private sectors in corroborating identity documents, especially as AI-based technologies are able to create increasingly realistic examples. It was agreed that enabling the industry to verify UK identity documents, such as passports and driving licences, should be a priority. Furthermore, access to these sources of 'good data' could be used to help tune automated screening tools to better spot fakes and identity fraud at the onboarding stage.

Finally, given the volume of identity fraud in the public sector in relation to applications for grants and benefits, better information sharing between the private and public sector was seen as key. As a minimum, there is a strong case for sharing known false and FOG identity document information between the public and private sectors, and participants pointed out that this could easily be done within existing data-protection legitimate interest and proportionality guidelines.

25. For example, see UK Identity Fraud Advisory, 'About Us', <https://www.ukifa.co.uk/about>, accessed 21 November 2024.
26. IDCARE is a charity that provides identity repair support to victims of identity theft and cyber attacks. It is funded by a cross section of public and private actors, including the Australian government. See IDCARE, <https://www.idcare.org/>, accessed 13 November 2024.

Recommendation 8: Law enforcement should consider a pilot to share with industry live operational non-identity attributes related to identity theft and fraud.

Recommendation 9: The UK government should work with industry to develop real-time UK government-issued identity-checking solutions and provide a data feed to industry on false identities used to access public funds.

Conclusion

The roundtable discussion highlighted the significant growth in recent years of the identity fraud threat, fuelled by the increased use of digital and online services. Enabled by large-scale data leaks, criminal marketplaces and the increased use of AI, identity fraud has a significant impact on both consumers and businesses, facilitating many types of serious criminality.

Although no single key intervention can be identified to respond to the threat, the roundtable participants discussed a number of existing interventions that could be scaled and key gaps that must be filled in a future fraud strategy. At the heart of the response must be a better collective understanding of the nature of the threat and increased knowledge and data connectivity between actors on the frontline of tackling the threat in the public and private sectors.

About the Authors

Kathryn Westmore is a Senior Research Fellow at RUSI's Centre for Finance and Security, where she leads the Centre's work on financial crime policy. Prior to joining RUSI, she spent 15 years as a financial crime consultant advising clients on issues related to fraud, bribery and money laundering. She served as a Specialist Advisor to the House of Lords Committee on Digital Fraud in 2022 and to the Home Affairs Select Committee's inquiry into fraud in the UK in 2023/24.

Helena Wood is the Director of Public Policy and Strategic Engagement at Cifas, the UK's largest not-for-profit fraud prevention membership organisation. She is an Associate Fellow at RUSI's Centre for Finance and Security, where she was previously a Senior Research Fellow and Head of the UK Economic Crime Programme. Earlier in her career, Helena spent over a decade in public service in the UK, with positions at the National Crime Agency, the Asset Recovery Agency, HM Treasury and the Charity Commission.