Fraudulent times: Identifying a consensus for an agenda to beat fraud

BRIEFING PAPER

October 2023

By Richard Hyde, Senior Researcher

We are in the midst of a fraud emergency. But efforts to tackle it have consistently fallen short of reversing its growth in recent years. A more concerted and long-term effort against fraud is needed. This requires a more cooperative approach by all those involved in the fraud chain and between the public and private sectors.

KEY POINTS

- In March 2023, the Social Market Foundation (SMF) and Stop Scams UK co-convened an expert roundtable with senior politicians, policymakers and regulators representatives from the financial, telecoms and technology industries, as well as consumer and business groups.
- Stop Scams UK organised a follow-up expert roundtable in June 2023 following the publication of the UK government's Fraud Strategy to look at what more needs to be done.
- The discussions at the two roundtables reflected the emergence of a possible consensus on how to better fight fraud.
- Opinion coalesced around a "whole eco-system" approach, whereby all organisations in the fraud chain as well as relevant policymakers, regulators and law enforcement take collective responsibility for tackling fraud and work proactively and cooperatively to beat it.
- The "whole eco-system" approach needs to be built on the foundations of significantly improved cooperation across the fraud chain and between the appropriate parts of the public and private sectors, which in-turn is dependent on the right leadership from the top of government and across industry.
- This approach has a number of components, which include:
    - Creating a better intelligence picture e.g. through enhanced data sharing across those sectors most impacted by fraud and between the public and private sectors, and the swiftest possible dissemination to those entities that can utilise it best.
    - More proactive prevention activity by banks, digital platforms, telecoms companies and others.
    - Improved consumer education efforts with greater reach across the population.

Kindly sponsored by

- The roundtable identified a number of obstacles to be overcome if the "whole eco-system" is to work, including:
    - The low prioritisation of fraud by organisations in the fraud chain as well as regulators and law enforcement, and the siloed nature of many of the current counter-fraud efforts.
    - Incompatibilities in technology and other organisational factors that inhibit cooperation e.g. the lack of capability and capacity for data sharing and intelligence dissemination in both industry and the public sector. Consequently, considerable investment is likely to be required to build them up.
    - Legal obstacles that inhibit the data sharing that is needed. The UK's data sharing framework does not sufficiently encourage proactive and extensive data sharing and intelligence dissemination across industries and between the public and private sector.
    - The adaptability of the criminals and their exploitation of new technologies which keeps them a step ahead of those trying to prevent or pursue them.

AREAS FOR ACTION BY POLICYMAKERS

- Help the organisations in the fraud chain take more concerted anti-fraud action by encouraging and facilitating improved coordination of the industry response to fraud against the UK.
- Increase consumer understanding of fraud and encourage greater levels of "fraud hygiene" among the public.
- Build a more accurate picture of the fraud threat to inform better policymaking.
- Anticipate and get ahead of new and emerging fraud threats.

INTRODUCTION

Two expert roundtables

In March 2023, the Social Market Foundation (SMF) and Stop Scams UK co-convened an expert roundtable on the issue of fraud. It was attended by politicians and policymakers from numerous government departments, regulators, academics, representatives of the financial services, telecoms industries and from a number of the major online platforms, as well as consumer and business interest groups. The aim of the roundtable was to explore the possibility of finding common ground about how to best to tackle the UK's fraud emergency.

In June 2023, Stop Scams UK convened a second roundtable. Again, participants included politicians and policymakers from government departments, representatives from regulators and the financial services and telecoms industries and several of the big digital platforms. Consumer and business groups also took part. This roundtable aimed to build upon the conversation at the first event, in light of the publication of the government's Fraud Strategy in May 2023.[1]

Signs of a growing consensus on how to better tackle fraud

This paper primarily aims to summarise the key themes discussed at the two roundtables. Emerging from the discussion was evidence of a degree of consensus among many of key people and organisations with an interest in the fraud issue, about how to better tackle the fraud emergency facing the UK.

Structure of this paper

Reflecting the contours of the discussions at the two roundtables, this paper:

- Establishes the scale of fraud committed against the people of the UK and highlights the evidence on the size of its impact on society.
- Describes some of the most commonly identified flaws in the current response to fraud and how ineffective it has been to date.
- Points out that the recently published UK government Fraud Strategy is a step forward but falls short of the kind of transformation needed to bring about a much more effective response to the problem of fraud.
- Outlines some of the key components of the "whole eco-system" counter-fraud approach, around which there was abroad consensus at the two roundtables.
- Sets out the kinds of obstacles that the participants in the two roundtables described as being hinderances to implementing a "whole eco-system" approach to tackling fraud.
- Suggests the kinds of steps that should be taken in order to successfully implement a "whole eco-system" approach and in-turn make a substantial positive difference to the current fraud problem.

THE IMPACT OF FRAUD ON THE UK

The scale of the fraud problem

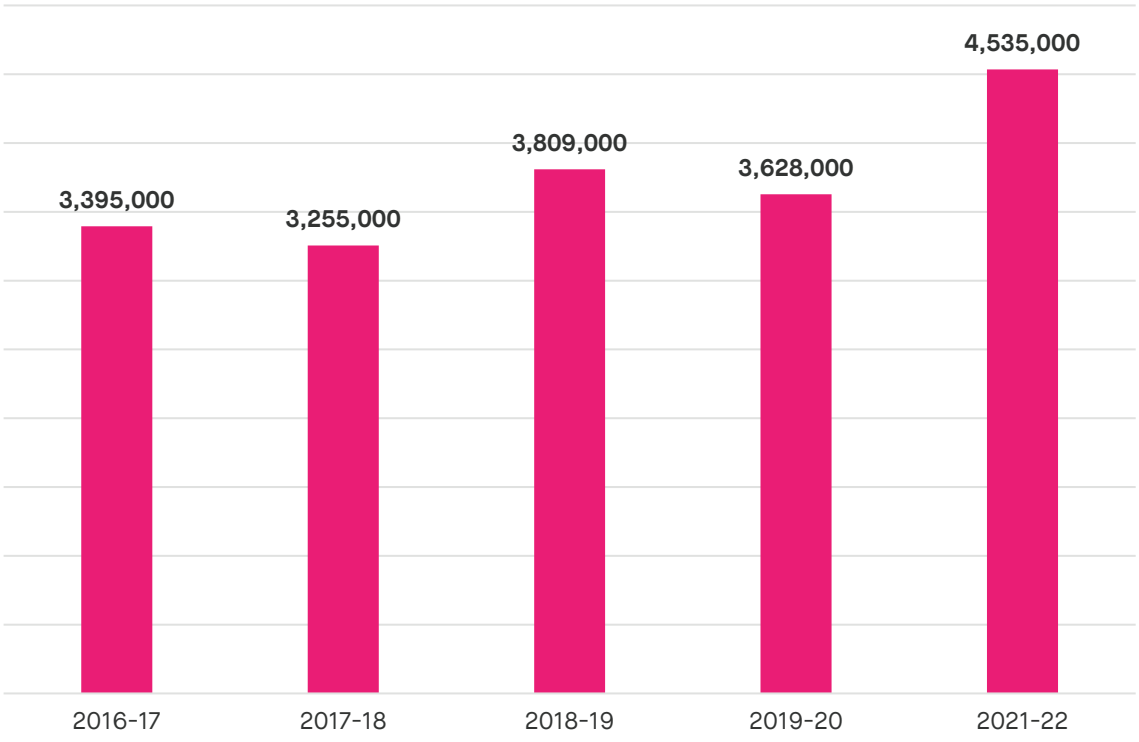
The scale of fraud perpetrated against individuals in the UK

Fraud has grown substantially in recent years. It now accounts for over four in ten of the crimes committed against individuals in England and Wales. One contributor to the first SMF and Stop Scams UK roundtable described the core of the problem vividly:

> *"...we are facing an enormous problem, it's being carried out by international criminal gangs with vast sums of money to invest, to commit crime...our online...telecoms and banking networks are being attacked by billions and billions of attempts...if only 10%...get through, that's going to cost billions for good people...".*

Figure 1 illustrates the trend in the number reported frauds perpetrated against people living in England and Wales between 2016-17 and 2021-22.

Figure 1: The scale of fraud against the people of England and Wales, 2017-18 to 2021-22



Source: CSEW 2016 – 2022

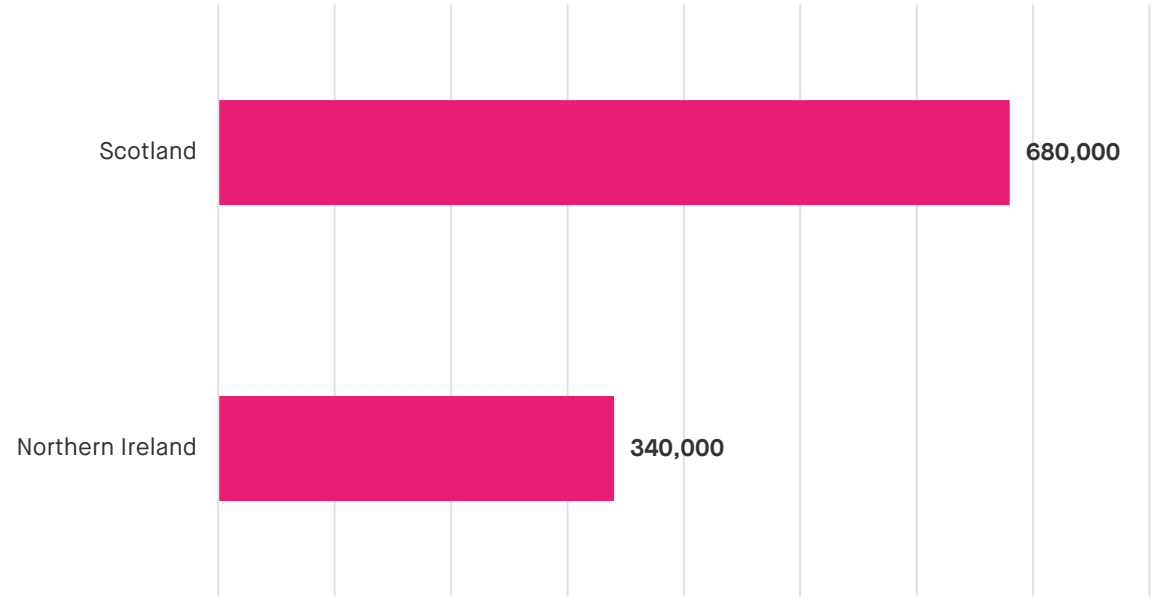
Box 1: Some of the key drivers of the fraud emergency

The growth of fraud has been, in part at least, a result of criminals switching away from higher risk crimes towards lower risk but lucrative offences such as fraud.[2] That reduced risk is the result of a number of factors but chief among them are:

- The low likelihood of a fraudster being successfully arrested and prosecuted. While there are various estimates of quite how low the ratio of criminals charged to frauds committed is, The Police Foundation has suggested that 0.6% of recorded frauds and 0.1% of frauds, as measured by the CSEW, end up in a charge or summons.[3]
- The development of digital networked technologies. The internet, for example, has created new vectors of attack for criminals and reduced the barriers to entry for both new fraudsters and for existing perpetrators to expand their criminal enterprises, whether they be domestic or based overseas.

Using the latest available data, Figure 2 shows the scale of reported fraud committed against the people of Scotland and Northern Ireland in 2019-20.

Figure 2: The scale of fraud against the people of Scotland and Northern Ireland, 2019-20



Source: Scottish Crime and Justice Survey 2019-20 and Northern Ireland Safe Community Survey, 2019-20

Estimates of the societal cost of fraud

Counting the cost of fraud to society

There are many estimates of the cost of fraud to the UK.[4] The cost is dependent on factors such as the victim group that is being measured and whether, how and which wider (i.e. second round) impacts are included. The latter are difficult to quantify (see Box 2). This increases the uncertainty around attempts at quantification of the costs.

One of the most robust estimates comes from the Annual Fraud Indicator (AFI). Its most recent analysis estimated that in 2022, the total cost to the UK of all fraud (i.e. against individuals and the public and private sectors), could be as high as £219 billion.[5] This was up from £190 billion in 2017.[6]

The societal cost of fraud against individuals

The recent Fraud Strategy published by the government suggested that in 2019-20 fraud against individuals in England and Wales cost society around £6.8 billion.[7] A recent paper from the SMF put the societal cost of fraud committed against individuals in the UK in 2021-22 in the region of £12.8 billion.[8]

Box 2: The negative impacts of fraud that are difficult to quantify

The government's Fraud Strategy has acknowledged the wider and deeper (but less measurable) costs to individuals and society that accrue from the prevalence of fraud. However, the problem of poor data and the intangible nature of some of the costs which can take a long time to emerge, make most analysis of the total societal cost of fraud underestimates.

These additional often intangible detrimental impacts include:

- The relative economic impact on individuals and families of being a fraud victim, e.g. 31% of fraud victims between 2020 and 2023 described the incident as having a "major" impact on their economic circumstances.[9]
- The psychological and social harms suffered by victims, which are difficult to quantify.[10] [11] Nevertheless, recent research suggested that 70% of victims between 2020 and 2023 experienced at least one second round impact. These impacts ranged from declines in self-confidence and mental health issues, through the need to claim welfare benefits or go into debt as a result of the fraud, to physical health and relationship problems.[12]
- The slow erosion of the rule of law while fraud remains *de facto* decriminalised, as a result of the decline of trust and confidence in the law and the institutions tasked with upholding it[i] [13] and the subsequent damage to the country's social and cultural capital.[ii]
- The close links between fraud and other serious crimes such as terrorism, modern slavery, human[14] and drug trafficking and money laundering,[15] [16] among others.
- The impact on the integrity of the UK's financial system and the consequences for the cost of and ease of access to consumer financial products.[17]

[i] There are already signs of this trend, as only a minority of fraud victims report their incident to Action Fraud, in large part due to the absence of faith in the police to deal with it. In-turn those that do report their incident to the police frequently report a poor experience. Source: House of Commons Committee of Public Accounts, 'Progress Combatting Fraud', Session 2022–23, 2023, https://committees.parliament.uk/publications/34609/documents/190751/default/.batting

[ii] The obvious and ongoing inability of the law and its associated institutions to deliver sufficient levels of security for citizens will undermine the rule of law and consequently diminish its role in fostering social cohesion and underpinning economic prosperity, such that both of these essential aspects of life in the UK will decline, potentially irreversibly so. Sources: Sanjai Bhagat, 'Economic Growth, Income Inequality, and the Rule of Law', *SSRN Electronic Journal*, 2020, https://doi.org/10.2139/ssrn.3736171.; Johannes Buggle, 'Law and Social Capital: Evidence from the Code Napoleon in Germany', *European Economic Review* 87 (2016), https://doi.org/10.1016/j.euroecorev.2016.05.003.; Krzysztof Głowacki et al., 'The Rule of Law and Its Social Reception as Determinants of Economic Development: A Comparative Analysis of Germany and Poland', *Law and Development Review* 14, no. 2 (2021): 359–400, https://doi.org/10.1515/ldr-2021-0043.

Business victims of fraud

Businesses are also victims of fraud. The Economic Crime Survey 2020 found that nearly one in five businesses (18%) had been victims of a fraud in the preceding three years.[18] This equates to nearly a million businesses.[19] However, the true annual cost to private sector is unknown, but one estimate suggests the losses in 2022 could have been as high as £157.8 billion.

THE PROBLEMS WITH THE CURRENT RESPONSE TO FRAUD IN THE UK

The current response is proving to be largely ineffective

The response to the growth of fraud against the UK has, so far, fallen short of what is needed to reverse its growth. This is evident in the scale of the fraud being perpetrated year-on-year and the quantum of societal costs that it continues to generate (see preceding section).

Many of the failings of the counter-fraud effort have been documented by the National Audit Office (NAO)[20] in its report "*Progress in combatting fraud*" in 2022[21] and by the House of Lords Fraud Act 2006 and Digital Fraud Committee.[22] The latter published its report "*Fighting fraud: breaking the chain*" in November 2022.[23]

The specific failings identified by the National Audit Office

The NAO noted in their most recent analysis of the Home Office's efforts to tackle the fraud problem, that:

- There was an absence of a coherent and concerted "whole-government approach" towards fraud.[24]
- Government's efforts have lacked clarity of purpose and that much of the activity that was taking place was incoherent, e.g. the NAO pointed to insufficient coordination with the private sector and inadequate leveraging of the private sector's expertise and capacity to help deal with fraud.
- Significant gaps in the availability and quality of data about fraud were inhibiting good policymaking and constraining the efforts of law enforcement.

The problems found by the House of Lords Fraud Act 2006 and Digital Fraud Committee

The disjointed counter-fraud landscape hinders effective action

The House of Lords Fraud Act 2006 and Digital Fraud Committee highlighted the "mind-boggling" array of organisations with an interest in fraud and described this disjointed landscape as a serious hindrance to concerted counter-fraud activity.[25]

The problems with the law enforcement response to fraud

The committee criticised the poor organisation of the law enforcement effort against fraudsters. They observed that there was a lack of leadership, focus and coordination had enabled the growth of "a vacuum" where there should be organised law enforcement action.

The committee suggested that the leadership and organisational problems with the law enforcement response to fraud were being compounded by significant under-resourcing.[26] The result has been and continues to be a persistent and substantial deficit in policing and prosecution capability and capacity in the fight against fraud.

Inadequate private sector effort is contributing to the scale of the fraud problem

The committee also examined the complexity of the private sector landscape. It described the fraud chain, noting that it can be long and complicated, involving a wide range of actors. These include telecoms networks, digital services providers (e.g. social media companies and web hosting services, etc), the professional services sectors, and the financial services industry. Each has a role in the fraud chain because, either fraudsters can and do utilise their services to commit fraud or, in some cases, they actively or passively enable fraudsters to launder their criminal gains. The committee's report further recognised that there are insufficient incentives for these private sector organisations to prioritise fraud and implement the kinds of measures that would help dramatically reduce it.

DOING BETTER IN THE FUTURE

The recently published government strategy

In May 2023 the government published its Fraud Strategy (Box 3). After various failures over the past decade to get to grips with the growing fraud problem, the strategy is the latest attempt to bring about improvements in the efficacy of the UK's counter-fraud efforts.

Box 3: Key facets of the government's Fraud Strategy

The UK Fraud Strategy has a number of components. It sets out an ambition to reduce the number of fraud incidents by 10% by the end of the current Parliament, from its 2019 pre-COVID levels. Specific measures it proposes to help achieve this include:

- Banning financial products cold calling, prohibiting SIM farms, and exploring action against the use of mass text aggregators and making it harder to "spoof" UK numbers.
- Making it easier to tackle fake companies, take down fraudulent websites, requiring the technology sector to introduce additional protections for their customers, and making it simpler for consumers to report fraud on platforms.
- Strengthening the reimbursement regime for victims.
- Replacing Action Fraud with a new reporting service.
- Improving intelligence sharing between private sector organisations in the fraud chain and the public sector and law enforcement.
- Bringing UK intelligence agencies into the fight against fraud.
- Making fraud a Strategic Policing Requirement (SPR) and establishing a new National Fraud Squad, involving officers from the National Crime Agency (NCA) and the City of London Police (CoLP) as well as Regional Organised Crime Units (ROCU).
- Increasing the penalties for fraudsters and examining ways the criminal justice process can be improved when dealing with fraud cases.
- Boosting international engagement on the topic of fraud, e.g. through hosting a global fraud summit in 2024 to help build an international consensus, reflecting previous efforts on issues such as child sexual abuse and exploitation.
- Overhauling the current approach to consumer awareness raising and information about fraud.

Source: Home Office. (2023). Fraud strategy: stopping scams and protecting the public

A step forward but insufficient to make a substantial difference to the fraud emergency

The strategy is a step forward if the measures it proposes are implemented effectively and they then deliver as they are expected to.[iii] Nevertheless, for substantial and sustained reductions in fraud to occur, the strategy falls short of the step change that is needed in the current approach. For example, the strategy is not ambitious enough in:

- Dealing with the long-standing problem of the disjointedness of the "mind-boggling array" of organisations with an interest in fraud, which constrains coordinated action.
- Pushing for greater levels of cooperation among organisations in the fraud chain and between the public and private sectors, not least in the area of data sharing across and between industries as well as with public bodies, and the concomitant generation and use of intelligence to both prevent fraud and pursue fraudsters.

KEY FACETS OF AN IMPROVED APPROACH TO TACKLING FRAUD

Signs of an emerging consensus over a way forward for tackling fraud

It was notable that, amongst most of those participating in the two expert roundtables, which this report is a brief overview of, there were clear signs of a broad consensus about what to do about fraud. It centred around the need to develop a "whole eco-system" approach.

Through providing a short summary of the discussion that took place at the two roundtables, this paper outlines some of the key components of the "whole eco-system" approach. It also describes a number of the biggest barriers to implementing such an approach that were identified in the exchanges at the roundtables.

A successful approach to tackling fraud needs to align the interests and efforts of all those in the fraud chain along with relevant parts of the public sector

Leadership and cooperation among all the parties in the fraud chain is a prerequisite for effective action

At both roundtables there was general agreement from attendees that success against fraud could only be achieved if the current approach (a multitude of separately devised and uncoordinated measures) was done away with and replaced by a holistic approach that all relevant parties were bought into. Two contributors to the first roundtable summed up the position succinctly:

[iii] In a 2019 review of the police response to fraud, HM Inspectorate of Constabulary (HMICFRS) described the previous 2006 fraud review and 2011 strategy as "forgotten". Source: Alan Doig and Michael Levi, 'Editorial: The Dynamics of the Fight against Fraud and Bribery—Reflections on Core Issues in This PMM Theme', Public Money & Management 40, no. 5 (2020): 343–48, https://doi.org/10.1080/09540962.2020.1752547.

> *"It's like Whack-a-Mole. We are all individually in our own silos, prioritising and making decisions, but they're all different. Therefore we're tackling this problem incrementally, not holistically, across the eco-system".*

> *"The eco-system approach…[means] stop[ping] working in isolation of each other. You're doing something different, you're doing something different. You're not going to achieve anything, so…we need to do it as a collective".*

It was pointed out at the two roundtables that the four key components of the "whole eco-system" approach (see more below) can only be delivered if there is a basis on which they can be put into action. This requires some essential foundations to be put into place first, including significantly enhanced cooperation across the fraud chain and between the appropriate parts of the public and private sectors (see pages 13–17 for more on obstacles to cooperation). In-turn, cooperation is reliant on the right leadership from the top of government and across industry, which can galvanise the relevant actors into:

- Seeing the problem sufficiently clearly.
- Aligning on the need to prioritise fraud and contribute to tackling it.
- Investing adequate time and resources into both individual organisation-level and collective actions to bring about a more effective overall response (there is more on the importance of leadership at the organisation level on pages 14-15).

Four key components of the "whole eco-system" approach

Prevention should be central to any counter-fraud agenda

The biggest priority for any counter-fraud effort, suggested by a number of participants in the first roundtable, should be prevention. This was seen as the main route to delivering the largest reductions in fraud. It was proposed by one roundtable contributor that this needed to involve building prevention into the digital services that consumers used:

> *"We have to focus upstream on designing a safe world for consumers, rather than hitting the problems as they pop up. [We need to] get to a position where consumers can be safe, rather than explaining what went wrong".*

Proactivity by the private sector, law enforcement and consumers is key to reducing fraud threats

For a coherent effort against fraud to make a substantial difference, it was argued that a proactive approach to the problem from all the key parties – both private and public – would be needed. The current approach was widely considered too reactive to events and trends. One roundtable attendee pointed out that fraudsters are adaptable and those looking to combat fraud, whether through prevention or pursuit, need to be "on the front foot" if there is to be a hope of tackling the fraud emergency:

> *"We're not on the front foot. We need to prioritise. We need a way to do it at pace, too".*

Developing actionable intelligence to prevent fraud and pursue fraudsters

Central to an active prevention effort and the successful pursuit of fraudsters is good intelligence.[27] Several contributors highlighted how essential data sharing is for intelligence purposes:

> *"Number one is data sharing, big data, that's where it would make a difference. Sharing across not in isolation, not once in-a while, no, it's got to be central".*

One contributor offered a taste of the kinds of data that needed to be shared:

> *"The modern world means that we need to share mobile intelligence, behavioural analytics, fraud signals, a whole group of other information".*

An intelligence-led approach requires the collection of high-quality data, the proactive and swift sharing of it among relevant people and organisations, and its effective collation and interrogation in order to provide actionable intelligence. Lastly and critically, it requires the dissemination of that intelligence to those who can take the appropriate actions.

Consumer education is important in reducing fraud risk

Equipping people with the right knowledge and tools to reduce their own fraud victimisation risk was also raised as a priority area at the first roundtable:

> *"We need to get people to take responsibility. You lock the front door, you don't leave it wide open for a burglar. We need to give them that same mindset".*

The potential gains from progress on this front are acknowledged in the government's Fraud Strategy.[28] However, as it was noted in the discussion at the first roundtable, many consumers show little concern for threats like fraud in their online behaviour, which increases the likelihood of them becoming victims:

> *"It's remarkable in a way that people are happy to go online and pay money...to someone they've never met, never seen, that they don't know exists. You wouldn't have done that with a property".*

This implies that consumer education will need to be carefully developed to ensure it can engender behavioural changes, away from what are often deeply entrenched habits amongst consumers.

MAJOR OBSTACLES TO TACKLING FRAUD MORE EFFECTIVELY

At the two expert roundtables it was noted that a "whole eco-system" approach faces a number of sizeable obstacles to its establishment, development and operation. These will need to be overcome, or at least substantially ameliorated, if such a response is to be implemented.

Different levels of buy-in from key partners

A significant barrier to the new approach that was identified at the first roundtable discussion was buy-in by those organisations that are part of the fraud chain as well as the relevant parts of the public sector. At the moment, levels of interest in fraud risks and the degree of proactivity towards dealing with fraud vary significantly between organisations and industries. Consequently, more cooperation will take greater levels of commitment from key parties in the first instance, supported by adequate resourcing and time for any changes to embed and be refined.

Clear leadership among organisations in the fraud chain and public sector is essential to taking fraud seriously

The importance of impetus from the top of organisations relevant to fraud was emphasised in the roundtable discussions. The leadership of a corporation for example, will dictate the level of interest in and commitment to issues. Fraud is but one of many that the leadership of a telecoms, digital services or financial services company for example, may have to consider.

It was noted at the second roundtable that the reality is, fraud will only ever be one factor among competing commercial priorities and a slew of legal obligations that fall on companies.[iv] The consequence is that the fraud threat, especially where the victim is not the business itself, is a comparatively low-priority issue, even when that organisation could play a prominent role in reducing the fraud risk to society:

> *"A lot of senior executives have a real paranoia about not having safeguards, exposing their organisations or conflicts with other obligations...[consequently]...I see a paralysis".*

The House of Lords Fraud Act 2006 and Digital Fraud Committee suggested that these leadership issues permeate the entire response to fraud. They are prevalent across the private organisations that are part of the fraud chain and the public sector, too. Evidence for the latter was observed by HM Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) in their evaluations of the polices' efforts against fraud.[29]

Leadership, it was argued by another participant, also has to come from regulators. They pointed out that the private sector is more likely to take an issue such as fraud seriously when regulators make it clear that it is keen that firms under their auspices do so:

> *"What matters is the will – and to get that, the regulator is critical, in that he [is] happy to see that type of activity".*

The obstacles to taking action

Information problems hold back coordination across the fraud chain

It was noted by several roundtable attendees that because each actor in the fraud chain can only see part of the whole picture:

[iv] These include actual or perceived trade-offs between effective counter-fraud measures on the one hand and preferences and obligations for privacy and data security on the other.

> *"You'll often see a fraud originating via one technology and the actual crime taking place on another, for example through a message, or they'll phone up".*

This partial information issue is a significant barrier to organisations being able to take counter-fraud actions:

> *"Other sectors have insights into that journey that we will never be able to have. We often see the initial kind of hook [the] banks have the other side of that picture, they see what happens at the end of that journey. If we can put those together we can mitigate those harms".*

A key part of the solution to the information problem is adequate data sharing among across the fraud chain and between the public and private sectors. However, implementing an effective system comes with costs and legal difficulties among other challenges.

The costs incurred for little direct benefit disincentivises action by actors in the fraud chain

The incentives for taking concerted counter-fraud action can also be weak while the disincentives are large, because taking action can be resource intensive and may generate little direct benefit to the organisation taking them.

The need to invest in people, processes and systems can hold back efforts to tackle fraud

The roundtable discussions highlighted a number of substantial cost-related disincentives that hinder counter-fraud activity such as greater cooperation across the organisations in the fraud chain:

- The first is the financial cost of making the relevant investments. For financial services firms in particular, further investment aimed at tackling fraud risk would come on top of that which they already spend on economic crime mitigation. For example, one estimate of the current cost of economic crime compliance to the sector suggested it was in the region of £34 billion a year.[30]
- The second aspect is that associated with the opportunity cost of dedicating resource to fraud when other ventures may deliver more obvious commercial returns.

These cost barriers are driven by:

- The large number of organisations involved and the cross-industry nature of the fraud chain (which implies a multiplicity of organisational structures, business models, and modes of operating) increase the difficulty and therefore the cost of cooperation.
- The volume of data that will need to be shared and collated, analysed and turned into intelligence and the extra computing capacity that will be needed to handle it.
- The presence of legacy systems in some industries and organisations means that some will struggle to play their part without significant modernisation of their systems.[31] [32]

- The need to invest in re-skilling or upskilling people to develop and operate any new or expanded data collection and sharing and intelligence generation and dissemination, and integrating them into existing operations.

As one contributor to the roundtable argued, the practicalities are:

> *"More complicated for online because business models are completely different. Whereas, among banks business models are very similar".*

These difficulties are likely to multiply when the public sector is also included, which it must be if there is to be "whole eco-system" approach.[33] Legacy systems are a significant issue in the public sector.[34] The public sector also struggles with access to sufficient people with the right IT skills to develop and operate any new or expanded systems that used for data collection and sharing, intelligence analysis and dissemination.[35]

Legal frictions hampering sharing efforts

In addition to organisational and technical obstacles to a proactive approach to data sharing, there was some debate at the two roundtables about the legal barriers. At the second roundtable in particular it was argued that the revisions to the UK's data protection regime that are in the pipeline[36] are unlikely to provide adequate legal cover for the kind of proactive and deep intra-industry, cross-industry and public and private sector data sharing that is needed to make a sizeable and positive impact on the fraud emergency:

> *"There's probably [a] need to have more permissive legislation if we want to share. However, what we don't have right now is a mechanism understood by all the partners about what constitutes consent".*

The sophistication of fraudsters

Fraudsters are a moving target

The observation was made by participants in the two roundtables that, a further significant challenge for those looking to reduce incidents of fraud is the nimbleness of the fraudsters, e.g. they are often rapid adopters of new technologies and methods. One contributor observed that:

> *"Every time we introduce new technology the window of time before the scammers find a way through is becoming shorter and shorter. There is no way of avoiding that because of the amount of resource they're prepared to invest. We [are] always a few steps behind".*

New technologies are going to compound the existing fraud threat

Technology is a key reason why fraud has reached epidemic proportions across much of the world and against the UK in particular.[37] While new technology provides opportunities to better tackle fraud,[38] it also creates the prospect of increasing the fraud threat.

Technologies such as artificial intelligence (AI) and blockchain (in particular the growth of crypto assets) are likely to see more and more criminals trying to utilise them for nefarious purposes. They pose a particular challenge to those looking to reduce fraud levels.[39] A recently cited example by the Federal Bureau of Investigation (FBI), illustrated how AI is already a growing threat. It has been used to generate "synthetic content" such as deepfakes for "spear phishing" and "social engineering" purposes.[40]

Technologies such as AI are, however, double-edged. They may provide new opportunities for criminals, but they can also empower law enforcement, regulators and others fighting fraud. Their development and impact and how government and societies respond to their emergence therefore, need to be carefully considered. That work needs to begin now in order to get ahead of the problems.

STEPS THAT SHOULD BE TAKEN TO DELIVER THE BETTER RESPONSE TO FRAUD

Having identified some of the key components of the "whole eco-system" approach and highlighted some of the biggest obstacles standing in the way of implementing it, the discussion at the two roundtables touched upon more specific steps that would be needed to make it work.

Alignment of goals and effort

Aligning around a goal to meaningfully reduce fraud is an essential starting point

There was a general view that the starting point would need to be clear prioritisation of fraud first followed by an alignment of effort around the goal of reducing fraud. One roundtable participant observed:

> *"What we've got to do is make sure that what we're doing is collaborating on intent, not just on action, because, if we get the intent aligned, that at least we will make sure that our actions align, even if our policies are not always in exactly the same places".*

As the participant quoted above noted, cooperation in counter-fraud actions would be expected to follow the alignment around the same goal. Another contributor to the first roundtable made a similar point about what needed to be done:

> *"The key thing is aligning all of that work and all those priorities. Let's learn all those things...and work together collaboratively".*

Equally important is alignment between private sector actors in the fraud chain and relevant parts of the public sector

Alignment of effort and greater coordination between the private sector organisations that are part of the fraud chain and key public sector entities such as law enforcement, relevant regulators, and policymakers was seen as equally important. As a contributor noted, the problem is one that the public and private sectors have to deal with and therefore success or failure will depend on whether both can "stand together":

> *"We still consider it to be a public sector problem and a private sector problem. We need to break down silos because the same policies are attacking both sides".*

Data sharing and intelligence generation and dissemination

Data sharing needs to be inter-industry and between the public and private sectors

Data sharing is a key factor in developing high-quality and actionable intelligence about fraud.[41] The centrality of data sharing was reflected in what contributors repeatedly said at both roundtables.

One participant noted that, within the financial industry, there has been some improvement in data sharing. The CIFAS model was cited as evidence.[v] However, greater incentives, it was argued, could further improve the data sharing effort:

> *"The data is out there, we need the incentives to share it at scale and in real time. That's why CIFAS exists and banks have gotten good at sharing data with each other"*

The inter-industry sharing of information e.g. between digital platforms, telecoms companies and banks and building societies, and sharing between the public and private sectors was seen by many as particularly vital:

> *"Making it cross sector opens up possibilities. If we were to crack data sharing, I think it just opens up a whole world of other ideas".*

Effective data sharing between organisations in the fraud chain remains a significant gap in the current response to fraud.[42] As an illustration of this, a participant pointed out that:

> *"Too often organisations say we don't have to do this, we don't have to share. These enormous amounts of information need to be shared".*

At present, the efforts that are made were seen by a number of those at the two roundtables as not being of sufficient scale, not necessarily involving all of the most useful data when it did happen, and it was often not swift enough to make a difference.

In addition, the poor record of the public sector on data sharing both internally and with the private sector was raised as another substantial capability gap:

> *"[There is a] huge amount of good data in the public sector not shared, huge amounts of Information among law enforcement that is not shared".*

[v] In 2020, data sharing through CIFAS's National Fraud Database (CIFAS) is estimated to have saved businesses over £1bn by helping prevent successful fraudulent activity. Source: Department for Business and Trade et al., 'Factsheet: Information Sharing Measures', Policy paper, 2023, https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/fact-sheet-information-sharing-measures.

Building on existing models to create more effective intra and inter-industry and public–private sector data sharing

It was argued at the second roundtable by two attendees that in order to bring about the most effective data sharing arrangement among financial services, telecoms companies, digital platforms, law enforcement and regulators, existing models with a proven record should be expanded:

> *"...a coalition of the willing and a partnership to see what the data could tell us...".*

> *"Get a small coalition of those who want to and then work their way to bigger...".*

Another followed-up to reinforce the point by adding that any system that is developed should avoid letting the perfect be the enemy of the good. A fourth participant noted working examples from other areas such as anti-money laundering (AML) and advocated learning lessons from them.

Reforming the law to bring about proactive data sharing across industries and between the public and private sectors

Any improved approach to data sharing (and in-turn intelligence generation and dissemination) will require the right legal framework to support it. At the second roundtable there was debate over the extent to which planned changes to current data protection rules will enable the kind of extensive and deep data sharing that is needed to make a substantial impact on fraud. [43] [44] Some at the roundtables believed that the changes may result in an incremental improvement but also noted its likely limitations:

> *"The legislation that's coming through is going to improve sharing information where we are already on notice of something, but not that other data sharing. It won't do cross sector, it only does it within the sector. And it only does it for those who are already willing to do it".*

In light of the likely limited impact, there was a view among many of the participants that the best policy for maximising the contribution of data sharing is to mandate it:

> *"It needs to be encouraged, it needs to be mandated. Only when the fear of not sharing exceeds the fear of sharing will we succeed".*

> *"It has to be mandated because you're only as strong as your weakest link. It only takes one platform, one telco or one bank not to play ball and that is the loophole that gets exploited".*

To de-risk the maximalist data sharing approach, for those involved in it, one contributor proposed the creation of an explicit "safe-harbour" protection:

> *"It's in the pursuit of protecting consumers, then we should be compelled to do it. But we need to make sure we have a safe harbour, legislative framework to motivate".*

The same participant suggested that the compulsory data sharing approach should be buttressed by a broader duty to cooperate laid upon those involved in the fraud chain, to give a robust underpinning to cooperation:

> *"The second is the coordination. What we do, and in what order, needs to be coordinated and mandated across all sectors".*

Another participant indicated that a safe-harbour approach would encourage relevant businesses in the fraud chain to make the invest in technologies[45], people, and processes that are needed to maximise data sharing, noting that:

> *"[Both] the public and private have a huge amounts of data [that are] not shared, [yet] data is what we need to put into our system to prevent fraud. Get us that data and then we'll use our technologies to be able to prevent more fraud. If you have that safe harbour, we can crack that".*

Redesigning processes to introduce greater assurance in payments and transfers

One of the benefits of greater data sharing would be the fillip it would give to other measures that financial services firms such as banks, the digital platforms, and telecoms companies already utilise to varying degrees, to bear down on the fraud emergency.

Increasing the frictions in the financial system

It was argued at the first roundtable that a useful mechanism for helping prevent fraud would be more "frictions" in parts of the financial system:

> *"What this comes down to is friction in the system. It's not something that companies themselves love doing of course, but there is a level of that we have to accept".*

Slowing down the flow of monies and boosting the levels of assurance around the legitimacy of payments and transfers for example, was seen by a number of roundtable contributors as a helpful tool in the armoury of effective counter-fraud measures. Frictions can range from the outright blocking high-risk payments and transfers, through slowing payments and transfers down with cooling-off periods, to flagging possible risks to payees before payments or transfers are made.

There is evidence of considerable public willingness to have more frictions introduced into the payments system to reduce fraud risk. SMF's own survey found that 70% of the UK public and 73% of previous fraud victims are happy to accept such measures if they can limit fraud risks.[46]

Proactive blocking of suspected malicious material

There were also calls at the roundtable for the adoption of a more proactive approach by digital platforms, other relevant digital services providers and telecoms companies, where practical, to the blocking of suspect material and malicious activity:

> *"What if we just blocked everything like that? We all thought it was a crazy idea, then, fast forward five years [and] It's a simple measure that's worked. We need more simple initiatives like that, [for example] share malicious domains [and] they get blocked".*

The relative success of the blocking of fraudulent phone calls through a concerted effort by some of the UK's telecoms companies and the industry regulator was noted in the first roundtable discussion as a sign that such efforts can make a difference.[47] [48]

Supporting consumers to improve their "fraud hygiene" behaviours

A single coordinated approach to public messaging about fraud risks

The importance of action to help educate consumers about fraud risks and induce behavioural changes that will reduce fraud victimisation was raised at both roundtables. In particular, the lack of "cut through" by current messaging on fraud was noted. Consequently it was argued by some that there was a need for a more ambitious and consistent approach, under a single brand:

> *"It's also about how we communicate consumer education. [It would] be more effective if there was a single brand, delivering messages, that has the public status".*

Using all opportunities to inform current and future consumers about fraud risks

Achieving behaviour change through campaigns is difficult but possible.[49] A number of contributors to both roundtables suggested that education about fraud risks should be common and delivered through as many channels as possible to maximise reach across different demographics:

> *"Integrated education in schools, universities, workplaces, where people are and can listen to information. So often, education comes too late in the heat of the moment when people are in a hot state".*

> *"It's about educating the consumer. We should have it within education [and] public information available".*

WHAT NEXT?

This paper was commissioned by Stop Scams UK to highlight the discussions at two expert roundtables, which straddled the period of the publication of the government's Fraud Strategy. This summary makes clear that there is a tentative emerging consensus across a considerable proportion of the relevant parts of the public and private sector, about some of the key steps that need to be taken to reduce the UK's vulnerability to fraud and, as a result, bring about a meaningful and sustainable reversal in the numbers of fraud incidents perpetrated against the UK and a concomitant reduction in the societal costs the fraud emergency is generating.

To that end, set out below is the outline of a policy agenda that could construct and embed a "whole eco-system" approach in the UK, in order to substantially reduce fraud and its harms.

RECOMMENDATIONS

Help the organisations in the fraud chain take more concerted anti-fraud action

- **Sponsor the establishment of a single fraud authority body that can galvanise and help organise the private sector into greater levels of cooperation** over counter-fraud activities and independently evaluate the success of those cooperation efforts over time.
- Support, with public resources (reflecting the public benefits that will accrue from reduced amounts of fraud), the **improvement of cross-sector and public–private data sharing and intelligence dissemination**. The National Economic Crime Centre is likely to be the best forum for coordinating this given its current role in trying to facilitate cooperative efforts between different relevant actors relevant to economic crime.[50]
- Underpin the efforts to improve **data sharing with a mandate on firms in industries that are part of the fraud chain, as well as relevant parts of the public sector, to proactively share data and disseminate intelligence**. This will need to be complemented by creating a more unambiguous legal position, which provides safe harbour to de-risk such activity, where practicable.

Increase consumer understanding of fraud and encourage greater levels of "fraud hygiene"

- Develop a single **national consumer education** approach that the public information campaign will communicate, to ensure a clear and consistent message to the public about the fraud threat and effective "fraud hygiene" measures that individuals and families can take.
- Have the proposed **single fraud authority lead on the development and implementation of a national public information campaign** on fraud, in order to maximise the input and support of the private sector in its formulation and the roll out.

Build a more accurate picture of the fraud threat to inform better policymaking

- The Home Office and other relevant government departments, law enforcement, appropriate regulators and key actors in the private sector (including the single fraud authority) should undertake a **joint review of the current state of data collection** about fraud and fraudsters, with the intention of improving the accuracy and depth of what is collected. The ultimate aim should be a body of improved fraud-related metrics which can inform better policymaking and provide the basis for benchmarking the performance of counter-fraud activities and the organisations carrying them out. Further, the review should consider how developments in the ways that fraud is committed (e.g. AI-enabled fraud), might be best reflected in official data.

Anticipate and get ahead of emerging developments in fraud threats

- The Home Office, UK law enforcement, relevant regulators, charities and industries with an interest in fraud should establish a **joint and time-limited expert taskforce to investigate the likely future developments** in the fraud threat. It should have a remit to evaluate the ways in which new technologies are already changing the fraud landscape and are likely to change it further. It should also look to identify potential strategies for adapting the UK's response to those new threats. It should report before the international conference on fraud proposed by the UK government in the Fraud Strategy, so that its findings can help inform the conference's agenda.
- **Step up international engagement over fraud and aggressively push forward the ambition in the Fraud Strategy for a more global focus**, not only to spur greater cross-country cooperative efforts against current fraud risks but also to ensure such efforts **reflect probable future developments in the fraud threat,** e.g. the utilisation by fraudsters of technologies like AI.

ENDNOTES

[1] HM Government, 'Fraud Strategy: Stopping Scams and Protecting the Public', 2023, Tackling fraud and rebuilding trust (publishing.service.gov.uk).

[2] Tim Robinson et al., 'Annual Fraud Indicator 2023', 2023, https://www.crowe.com/uk/insights/annual-fraud-indicator.

[3] Strategic Review of Policing in England and Wales, 'A New Mode of Protection: Redesigning Policing and Public Safety for the 21st Century', Final Report, 2022, srpew_final_report.pdf (policingreview.org.uk).

[4] Richard Hyde, 'Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud on the UK', Social Market Foundation., accessed 11 September 2023, https://www.smf.co.uk/publications/impact-of-fraud-on-the-uk/

[5] Robinson et al., 'Annual Fraud Indicator 2023'.

[6] Robinson et al.

[7] HM Government, 'Fraud Strategy: Stopping Scams and Protecting the Public'.

[8] Richard Hyde and Peter Wilson, 'Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud on the UK', Social Market Foundation., accessed 11 September 2023, https://www.smf.co.uk/publications/impact-of-fraud-on-the-uk/.

[9] Richard Hyde and Peter Wilson, 'The View from the Ground: Building a Greater Understanding of the Impact of Fraud and How the Public View What Policymakers Should Do about It', 2023, https://www.smf.co.uk/wp-content/uploads/2023/09/The-view-from-the-ground-September-2023.pdf.

[10] Mark Button, Chris Lewis, and Jacki Tapley, *Fraud Typologies and the Victims of Fraud: Literature Review* (London: National Fraud Authority, 2009).

[11] 'Fighting Fraud: Breaking the Chain' (House of Lords: Fraud Act 2006 and Digital Fraud Committee, (12 November 2022).

[12] Hyde and Wilson, 'The View from the Ground: Building a Greater Understanding of the Impact of Fraud and How the Public View What Policymakers Should Do about It'.

[13] Luisa Blanco and Isabel Ruiz, 'The Impact of Crime and Insecurity on Trust in Democracy and Institutions', *American Economic Review* 103, no. 3 (2013): 284–88, https://doi.org/10.1257/aer.103.3.284.; Luisa Blanco, 'The Impact of Insecurity on Democracy and Trust in Institutions in Mexico' (RAND Corporation, 2012), https://www.rand.org/pubs/working_papers/WR940.html.; Angelo Cozzubo, Elard Amaya, and Juan Cueto, 'The Social Costs of Crime: The Erosion of Trust between Citizens and Public Institutions', *Economics of Governance* 22, no. 2 (2021): 93–117, https://doi.org/10.1007/s10101-021-00251-0. and Tista Mukherjee, 'Crime and Trust in Institutions: Evidence from India', *Applied Economics Letters*, 29 September 2022, 1–5, https://doi.org/10.1080/13504851.2022.2129564.

[14] Name Scan, 'INTERPOL's Warning: Human Trafficking-Fuelled Fraud on the Rise', 9 June 2023, https://insights.namescan.io/interpol-global-warning-human-trafficking-fueled-fraud/.

[15] EUROPOL, '228 Arrests and over 3800 Money Mules Identified in Global Action against Money Laundering', n.d., https://www.europol.europa.eu/media-press/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering.

[16] Sal Jadavji, 'Fraud and Money Laundering: What's the Connection?', *ACAMS Today*, 2 September 2011, https://www.acamstoday.org/fraud-and-money-laundering-whats-the-connection/.

[17] Refinitiv, 'Revealing the True Cost of Financial Crime: What's Hiding in the Shadows?', 2018, https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/true-cost-of-financial-crime-global-focus.pdf.

[18] Home Office, 'Economic Crime Survey 2020', 2023, https://www.gov.uk/government/publications/economic-crime-survey-2020/economic-crime-survey-2020.

[19] Richard Hyde and Peter Wilson, 'Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud on the UK', Social Market Foundation., accessed 11 September 2023, https://www.smf.co.uk/publications/impact-of-fraud-on-the-uk/.

[20] National Audit Office, 'Progress Combating Fraud', 2022, Progress combatting fraud (nao.org.uk).

[21] National Audit Office.

[22] Nicole Winchester, 'Tackling Fraud: Lords Committee Report', 14 June 2023, Tackling fraud: Lords committee report - House of Lords Library (parliament.uk).

[23] 'Fighting Fraud: Breaking the Chain' (House of Lords: Fraud Act 2006 and Digital Fraud Committee, 12 November 2022).

[24] National Audit Office, 'Progress Combating Fraud'.

[25] Winchester, 'Tackling Fraud: Lords Committee Report'.

[26] Winchester.

[27] Rick Brown et al., 'The Contribution of Financial Investigation to Tackling Organised Crime: A Qualitative Study', 2012, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/116518/horr65.pdf.

[28] HM Government, 'Fraud Strategy: Stopping Scams and Protecting the Public', 2023, Tackling fraud and rebuilding trust (publishing.service.gov.uk).

[29] HMICFRS, 'Fraud: Time to Choose - An Inspection of the Police Response to Fraud' (HMICFRS, 2019), https://www.justiceinspectorates.gov.uk/hmicfrs/publications/an-inspection-of-the-police-response-to-fraud/.

[30] Lexis Nexis, 'Report: True Cost of Compliance 2023', LexisNexis Risk Solutions | Transform Your Risk Decision Making, 2023, https://risk.lexisnexis.co.uk/insights-resources/white-paper/true-costs-of-compliance.

[31] 'Addressing the Problems of Legacy Banking Systems', *International Banker*, 26 October 2020, https://internationalbanker.com/technology/addressing-the-problems-of-legacy-banking-systems/.

[32] Vlad Vahromovs, 'Legacy Systems in Banking: The Major Barrier for Digital Transformation', *Fintech Futures*, 22 November 2021, https://www.fintechfutures.com/2021/11/legacy-systems-in-banking-the-major-barrier-for-digital-transformation/?ref=nanonets.com.

[33] Nick J Maxwell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', Occasional Paper, 2017, https://static.rusi.org/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwwell_artingstall_web_4.2.pdf.

[34] Damien Venkatasamy, 'Government Legacy IT Systems Holding Back Public Sector Transformation', *Civil Service World*, 26 August 2014, https://www.civilserviceworld.com/in-depth/article/government-legacy-it-systems-holding-back-public-sector-transformation.

[35] Department for Digital, Culture, Media and Sport and Department for Science, Innovation and Technology, 'Quantifying the UK Data Skills Gap - Full Report', 2021,

https://www.gov.uk/government/publications/quantifying-the-uk-data-skills-gap/quantifying-the-uk-data-skills-gap-full-report.

[36] Adam Clark et al., 'The Data Protection and Digital Information (No. 2) Bill 2022-23', 28 March 2023, https://commonslibrary.parliament.uk/research-briefings/cbp-9746/.

[37] Mark Button and Cassandra Cross, 'Technology and Fraud: The "Fraudogenic" Consequences of the Internet Revolution.', 2017.

[38] Darrell M West, 'Using AI and Machine Learning to Reduce Government Fraud' (Brooking Institution, 10 September 2021), https://www.brookings.edu/articles/using-ai-and-machine-learning-to-reduce-government-fraud/.

[39] Mark A. Nickerson, 'Fraud in a World of Advanced Technologies The Possibilities Are (Unfortunately) Endless', *The CPA Journal*, July 2019, https://www.cpajournal.com/2019/07/01/fraud-in-a-world-of-advanced-technologies/.

[40] Federal Bureau of Investigation, 'Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations', 10 March 2021, https://www.ic3.gov/Media/News/2021/210310-2.pdf.

[41] Kathryn Westmore, et al., 'Enabling Cross-Sector Data-Sharing to Better Prevent and Detect Scams', 2022, https://static.rusi.org/347_CR_Preventing_Scams_proof%20final.pdf.

[42] Kathryn Westmore, et al., 'Enabling Cross-Sector Data-Sharing to Better Prevent and Detect Scams', 2022, https://static.rusi.org/347_CR_Preventing_Scams_proof%20final.pdf.

[43] Adam Clark et al., 'The Data Protection and Digital Information (No. 2) Bill 2022-23', 28 March 2023, https://commonslibrary.parliament.uk/research-briefings/cbp-9746/.

[44] Payments Strategy Forum, 'Financial Crime Data and Information Sharing Solution: Proposed Approach and Outline Project Transfer Document', 2017, https://www.psr.org.uk/media/xmsnkocd/financial-crime-data-and-information-sharing.pdf.

[45] Yang Bao, Gilles Hilary, and Bin Ke, 'Artificial Intelligence and Fraud Detection', in *Innovative Technology at the Interface of Finance and Operations*, ed. Volodymyr Babich, John R. Birge, and Gilles Hilary, vol. 11, Springer Series in Supply Chain Management (Cham: Springer International Publishing, 2022), 223–47, https://doi.org/10.1007/978-3-030-75729-8_8.

[46] Richard Hyde and Peter Wilson, 'The View from the Ground: Building a Greater Understanding of the Impact of Fraud and How the Public View What Policymakers Should Do about It', 2023, https://www.smf.co.uk/wp-content/uploads/2023/09/The-view-from-the-ground-September-2023.pdf.

[47] Ofcom, 'New Ofcom Rules to Fight Fake Number Fraud', 15 November 2022, https://www.ofcom.org.uk/news-centre/2022/new-ofcom-rules-to-fight-fake-number-fraud.

[48] Home Office, 'Fraud Sector Charter: Telecommunications', GOV.UK, 21 November 2022, https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter.

[49] Catherine Mann, 'Behaviour Changing Campaigns: Success and Failure Factors', 2011, https://www.transparency.org/files/content/corruptionqas/270_Behaviour_changing_campaigns.pdf.

[50] Helena Wood, 'Five Problems with Economic Crime Policing – and How to Solve Them', 11 July 2022, https://rusi.org/explore-our-research/publications/commentary/five-problems-economic-crime-policing-and-how-solve-them.