It Could Be You

Stemming the tide of financial fraud in the UK

A Policy Network Special Report

Tom Startup, Charlie Cadywould and Matthew Laza
November 2017
Contents

1. Executive summary 4
2. Introduction: A modern epidemic 6
3. Key findings 8
4. Recommendations 30
5. Glossary 39

About the Authors

Tom Startup is a researcher and writer on economics and government policy. Formerly head of public sector research at Deloitte and a senior policy analyst at the prime minister’s strategy unit, he has published reports on poverty, property taxation, local government and private finance initiative, as well contributing to government white papers. His most recent report, Making the Most of Brexit, analysed the potential impact of Brexit on different regions of the UK.

Charlie Cadywould is a researcher at Policy Network, leading its progressive futures programme. Prior to joining, he was a researcher at Demos, authoring numerous publications on social and economic policy including Banking for All, on tackling financial exclusion in the UK. He holds a BA in social and political science from the University of Cambridge and an MSc in public policy from University College London.

Matthew Laza is the director of Policy Network and an experienced broadcast journalist who spent more than a dozen years as a BBC current affairs programme maker, including as series producer on Rip Off Britain before becoming a senior adviser to the UK leader of the opposition in the run up to the 2015 election. Before entering television he led the main Labour party pro-European organisation, campaigning for Britain’s leading role in Europe.
About this report

This report was commissioned by NatWest. It focuses on financial fraud (including scams) as experienced by individuals and consumers in the UK, particularly where that fraud has been enabled through computers or the internet. It does not seek to analyse fraud where the target was an organisation (public or private), or the kinds of frauds where money is not the primary motive.

Research for this report involved a review of the data available and literature on fraud and scams, both in the UK and abroad, new analysis of YouGov survey data, and interviews with domestic and international stakeholders and fraud experts.

The views expressed in this report represent those of the author and not necessarily those of NatWest. Any omissions and errors are solely the authors' own.

Acknowledgements

The authors would like to thank NatWest for financially supporting the research, as well as – led by Paula Dyke – sharing their technical expertise and support.

In addition to this, our thanks go to Conor Pope and Policy Network colleagues Josh Newlove, Alex Porter, Katherine Roberts, Sam Sigere and Sophia Dietrich, who have also provided invaluable assistance in the research, editing and production stages of the report.

We would also like to thank the following people who kindly agreed to be interviewed as part of this research. The conclusions of the report remain the sole responsibility of the authors.

- Louise Baxter, team manager, National Trading Standards Scams
- Professor Mark Button, director of the Centre for Counter Fraud Studies, University of Portsmouth
- John Crombez, former minister against fraud, Belgium
- Simon Dukes, chief executive, Cifas
- Bruno Farinelli, head of operations, ClearSale
- Chris Felton, detective inspector, National Fraud Intelligence Bureau
- Jim Gee, head of forensic and counter fraud services, Crow Clark Whitehall/Centre for Counter Fraud Studies
- Phil Malwhinney, policy manager, Age UK
- Neil Masters, national lead for fraud and economic cyber crime, Victim Support
- Carl Miller, research director, Demos Centre for Analysis of Social Media
- Paul Naldrett, managing director, Idemia (formerly OT-Morpho)
- Tony Neate, chief executive, Get Safe Online
- Maarja Punak, web constable, Estonian Police
- Talal Rajab, head of cyber and national security, TechUK
- Delia Rickard, deputy chair, Australian Competition and Consumer Commission
- Jamie Thunder, senior policy advisor, Which?
- Glenn Wicks, deputy chief investigator, Department of Business, Energy and Industrial Strategy
- Katie Worobec, head of fraud and financial crime prevention, UK Finance
1. Executive summary

Financial fraud is now the most common crime in Britain, perpetrated in enormous numbers by organised criminals both domestic and international. It hits every part of society, but with most fraud now experienced online, younger generations – digital natives who are most likely to use the internet for banking, shopping and to share their details online – are now the most vulnerable. The threat includes criminals illegally accessing personal accounts and cards to steal money, as well as the subtler problem of scams, where the victim makes a payment under false pretences. Despite a range of initiatives – some more successful than others – government, financial institutions and others are still struggling to meet the challenge.

This paper describes how the nature of fraud (including scams) has evolved in recent years, and how government and law enforcement authorities have been tackling the problem. It offers a series of recommendations for governments, banks and others that could, if implemented, stem the tide of these crimes in the UK, better protect consumers and give them the confidence to surf, shop and securely send money online.

Key findings

- There is a common misperception that older people are most at risk from fraud. In fact, it is the younger ‘digital natives’ that are most vulnerable as these crimes have moved online.
  - 25-44 year olds are most at risk from fraud
  - 16-24 year olds are most at risk from computer misuse crime (e.g. viruses and hacking)
  - Under 21s are increasingly at risk of having their accounts used for illegal activity

- Incautious behaviour is putting digital natives at risk. Confidence using technology can easily slip into foolhardiness.
  - 29 per cent of 18-24 year olds are willing to share their mother’s maiden name online, compared to just 12 per cent of over 55s
  - Security is most lax on the devices disproportionately used by digital natives for banking and shopping
  - While 86 per cent would install security software on a PC, just 57 per cent and 50 per cent would do so on tablets and phones respectively

- For years, governments thought crime was falling; in fact, much of it has simply moved online.

- The government has started to respond, but there is a lack of clear accountability between various bodies.

- The criminal justice system has not yet adapted to these new threats.

- Banks have responded, but are hampered by existing technology, regulations and limited coordination.
Despite promising technological innovations, the response of the tech giants has been muted.

**We are calling on the government to:**

- Ensure the next generation of digital natives know how to stay safe online, stepping up online safety education and making all teenagers complete a short, online course in cyber security, fraud and scams before they leave school.

- Work with the Joint Fraud Taskforce to design and introduce a National Fraud Indicator and an ambitious target for fraud reduction – a 25 per cent reduction by 2025.

- Bring together existing resources into a new national Economic Crime Agency, with powers to investigate, disrupt and prosecute for fraud and scams.

- Require all companies to report data breaches – no loopholes or caveats.

- Invest more in victim-orientated approaches to disrupt scams through the use of financial intelligence.

**Law enforcement should:**

- Reallocate resources and staff into economic crime and introduce web constables.

- Make greater use of social network analysis in fraud investigations, which will require better data-sharing across government departments and agencies.

**The banking sector should:**

- Set up an industry-wide initiative to tackle card not present fraud by upgrading card technology.

- Encourage – both through innovative design and financial incentives – customers to choose a package of new, more secure, banking services which reduce the scope for APP scams.

**The telecommunications and tech sector should:**

- Work more closely with banks and government organisations to tackle the problem, joining the Joint Fraud Taskforce and spreading the anti-fraud message on their platforms.

- Make computers and phones more secure, by design.

**Government and the private sector must work together to:**

- Review how financial losses that result from APP scams should be allocated between consumers, banks, and telecommunications and technology companies.

- As has been achieved for in-branch transactions through the Banking Protocol, develop a new, step-by-step approach for tackling fraud and scams that take place via electronic transfers.
2. Introduction: A modern epidemic

Fraud and scams, as forms of deception, are as old as humanity itself. All that is required is for one person to deceive, trick or impersonate another and so steal from them. But for centuries these crimes were kept at bay by several factors: most people were poor so had little to steal while the rich were highly protected; people generally transacted only with people in their immediate locality who they knew; and money was physical, making it cumbersome for fraudsters to find and move. Significantly, without the existence of a substantial police presence, it was simply easier to steal or burgle. The result was that fraud was a mostly minor occupation.

But the social and economic changes of the last few decades have swept away these barriers. Economic advances mean many of us now have the incomes of latter day kings, but without the bodyguards to protect us, making us all potential targets. Meanwhile, globalisation means we can communicate with, and transfer money to, unknown people in any part of the world. And money is now almost entirely digital, not physical – for a transfer to take place often all that is required is a few taps on a smartphone. At the same time, modern police forces have continued to prioritise physical crime – displacing criminals into the more anonymous world of fraud and scams.

Box 1: Scams and frauds: A note on terminology

In ordinary language, the terms ‘scam’ and ‘fraud’ are roughly interchangeable. Both are intentional acts of deception, usually for the purposes of financial gain. However, the term ‘scam’ is often given a more specific meaning, referring to a situation where the fraudster has tricked the victim into making a payment themselves, albeit under false pretences. Other frauds, on the other hand, can be perpetrated without the victim’s knowledge or involvement.

Fraud has a clear status in law under the 2006 Fraud Act which defines three types: false representation (which would include scams), failure to disclose information, and abuse of position. Official statistics, including the Crime Survey of England and Wales, use the term ‘fraud’ as an umbrella term that includes ‘scams’. The term ‘scam’, on the other hand, has no clear legal meaning.

For banks, this distinction between transactions that were made with or without the account holder’s authorisation is crucial. Under consumer protection legislation, the victim of fraud conducted without authorisation would have the right to have their money reimbursed (provided they had not acted fraudulently themselves or been grossly negligent). For scams, where the victim has authorised the transaction, they are much less likely to be reimbursed because, from the bank’s point of view, the transaction was correctly authorised.

This report focuses on both categories (understood as above). ‘Fraud’ and ‘fraud and scams’ are used throughout as umbrella terms. Where the distinction between the two is important, we have made it clear in the text.
The impact, as this report argues, has been dramatic. Financial fraud has exploded, becoming the most common crime in Britain today. It is perpetrated in enormous numbers in the UK by organised criminals based around the world. But, by and large, the government and financial institutions are still struggling to contain this distinctly modern epidemic. The forces that have unleashed this epidemic will not go away any time soon. But there is still much that can be done to keep it at bay.
3. Key findings

The huge scale and impact of financial fraud in the UK is only just becoming clear

The decline in crime was once considered one of the most remarkable social trends of the last 20 years. The latest statistics from the Crime Survey of England and Wales show that prevalence of most types of crime have continued to fall since the peak in 1995. However, new experimental measures of the prevalence of ‘fraud’ and ‘computer misuse’ (see box 2) suggest that this supposed decline may, all along, have been skewed by the massive under-reporting by victims of financial fraud and cyber crime.

Box 2: The confusing picture of fraud and computer crime in the UK

How common are fraud and cyber crime in the UK? The answer is not as simple as you might expect. The most widely-used and reliable source of data on the prevalence of crime in England and Wales is the Crime Survey of England and Wales (CSEW). This is a survey of households asking them to report whether they have been victims of crime, and if so what type. However, that survey only asked a narrow set of questions mostly about card fraud, omitting other types of fraud and cyber crime.

This changed in 2015 when new questions were asked about different types of fraud and offences related to computer misuse. The latter refers to viruses and the accessing personal information without permission (e.g. through hacking), which can be used to carry out fraud. These results were included in the latest statistics for the first time, but are still considered ‘experimental’ and are likely to be refined in future surveys. However, because of this, it is not yet possible to provide a clear picture of the trend in such crimes.

The other main source of data is crime that has been reported to the police. The National Fraud Intelligence Bureau (NFIB) collates data from Action Fraud, CIFAS and FFA UK. This gives a different picture of the prevalence of such crimes. However according to the CSEW only 17 per cent of victims of fraud report it to the police. Furthermore, FFA UK only refer crimes to NFIB where there is actionable intelligence. This is why the crime survey, despite its provisional nature, remains the most reliable source of information.

According to the latest crime survey, there were around six million crimes last year. However, including fraud and computer misuse offences, this rises to over 11 million. In other words, the new category has generated a colossal 5.4 million additional offences that were previously unreported. If accurate it would mean fraud and computer crimes account for nearly half of all crimes, with offences affecting over four million people.¹,²


¹. This category includes various types of fraud, identity theft, and computer misuse.
Of these 5.4 million offences, 3.5 million are fraud. 2.8 million people, around six per cent of the adult population, say they were victims of fraud in the last year. Fraud is now the most common form of crime in the UK. It is twice as common as vehicle-related theft, nearly three times as common as domestic burglary and 25 times as prevalent as robbery.

Data from other sources confirm the scale of the problem. For instance, NatWest/YouGov survey data found that 16 per cent of people had experienced online fraud in the past year, and 10 per cent, online bank fraud. Rates of fraud as reported to the authorities are, as expected, much lower due to under-reporting (see box 2). The latest figures from UK Finance, the industry body, show that...
losses from bank card fraud for the first half of 2017 were down 11 per cent on the first half of 2016.\(^5\) However, the number of recorded cases was roughly the same (meaning average losses per incident were down). Moreover, the available figures for full years show rising losses every year since 2012, including a nine per cent rise between 2015 and 2016.\(^6\)

Even by international standards, the UK is a hotspot for fraud. The number of frauds per 1,000 inhabitants is 67.5 – the highest in the EU, and seven times the rate in Germany.\(^7\) In part, discrepancies across Europe reflect rates of transactions; countries like the UK where people use cards for the majority of transactions will see higher rates per inhabitant than those where cards are used more rarely. However, when we look at card fraud per transaction, the UK is second only to France, twice as high as in Germany and three times the rate in Spain.\(^8\)

Figure 3: Card fraud per transaction in EU states (2013)


Again, part of the explanation might be that criminals will tend to target areas where there is most money to be made, so countries such as the UK with more transactions taking place are particularly vulnerable. On top of this, it may be that English’s status as the global language makes English-speaking victims a particular target – a Romanian gang may be more likely to be able to scam in English than in Greek or Italian. Delia Rickard, deputy chair of the Australian Competition and Consumer Commission told us that “Scammers do seem to have a fondness for English language countries.”

By far the most common fraud relates to banks and credit accounts, followed by computer viruses, then non-investment fraud.

---


7. Ibid.

iii. Bank and credit account fraud comprises fraudulent access to bank, building society or credit card accounts or fraudulent use of plastic card details.

Computer virus comprises any computer virus, malware or distributed denial of service (DDoS) attack which infects the computer or internet enabled device.

Non-investment fraud comprises cases where the respondent has generally engaged with the fraudster in some way, usually to make a purchase which is subsequently found to be fraudulent, for example, online shopping, bogus callers, ticketing fraud, phone scams and computer software service fraud.

Unauthorised access to personal information (including hacking) comprises offences where the respondent’s personal details have been accessed without their permission.

Advance fee fraud comprises incidents where the respondent has received a communication soliciting money for a variety of emotive reasons, for example, lottery scams, romance fraud and inheritance fraud.


Source: Crime in England and Wales, Experimental Statistics (see notes on categories iii).
Fraud is not something that happens to ‘other people’ – it affects all groups in society, and the digital natives are most at risk

There is a persistent idea that the elderly are particularly at risk from fraud and online deception. 46 per cent of people surveyed by NatWest/YouGov thought that those over 66 years old were most at risk, while only three per cent of respondents chose the 26-35 age-group. However, according to the latest statistics, almost exactly the opposite is the truth: fraud disproportionately hits the younger half of the population, while 16-24 year olds are the group most at risk from computer crimes. Fraud can only be successfully tackled when the debate changes to focus on younger people.

All groups suffer from fraud, but those over 75 are least likely to be victims of all these offences. Fraud was most prevalent among those aged 25-34 and 35-44. Those in the 65-74 bracket are marginally more likely to be victims of fraud than 16-24 year olds.

Figure 5:

Source: Crime in England and Wales, Experimental Statistics.

Internal NatWest analysis of fraud across different customer groups paints a similar picture, though with fraud skewed even more towards younger people, they find that fraud is most prevalent among Young Potentials (18-34 yr olds, with modest incomes and mortgages) and University/Graduates (18-25 yr old students and recent graduates). For instance, there is a growing problem of young people being persuaded to give access to their bank accounts for fraud and money laundering. Sometimes criminals use social media sites to advertise ‘cash flips’, where young people get paid to allow their accounts to be used for illicit purposes. In the first half of 2017 misuse of facilities fraud – the use of bank accounts for fraudulent purposes – doubled among account holders under the age of 21.

One explanation for this pattern is simply that older people are online less. While nearly 100 per cent of those between 16 and 54 have used the internet recently, it’s only 78 per cent for those 65-74 and 41 per cent for the over 75s. So older people may be less likely to receive phishing emails or visit fake websites. Those most at risk (25-44 year olds) are both online a lot, and likely to have the incomes and wealth to attract fraudsters.

Another part of the explanation is that some victims are not aware of being scammed. Age UK report that 53 per cent of people over 65 have been targeted by scams and criminals. But many of
these victims may not be aware of it. Louise Baxter of the National Trading Standards Scams Team told us that older people who are suffering from dementia might be among those who have been defrauded for many years, without even realising it.

Fraud disproportionately affects those in employment, as well as those who have a temporary or long-term illness. For the employed, their higher risk probably reflects a combination of higher incomes than other groups, as well as their use of the internet. For those who are sick/ill, their higher risk may reflect the fact that they are vulnerable or more likely to be socially isolated than other groups.

Figure 6:

![Prevalence of fraud by employment status](image)

Source: Crime in England and Wales, Experimental Statistics.

The idea of fraud as ‘the rich man’s crime’ remains true to some extent. If you had an income over £50,000, there was a nine per cent chance you were a victim of fraud, nearly twice the risk facing the poorest people.  

---

Computer misuse crimes, on the other hand, show a somewhat different demographic pattern. These include computer viruses and unauthorised access to personal information, such as through hacking, which can then be used to steal, extort or scam money from the victim. Those most at risk of computer misuse crimes are the youngest – those between 16-24 – and the oldest are least likely. In our interview with Simon Dukes of Cifas, he told us that the fastest-growing victim group for identity fraud is the under-25s.

Source: Crime in England and Wales, Experimental Statistics.

Those most likely to suffer from these crimes are the unemployed, students and those suffering from ill-health. In the case of students this probably reflects their reliance on their computers and relative lack of caution online; in the case of the unemployed and sick it may reflect their vulnerability and possibly out of date hardware/software.
Finally, like fraud, computer misuse crimes are disproportionately targeted at richer people. Those earning over £50,000 per year are twice as likely to be targeted as those on the lowest incomes.

Source: Crime in England and Wales, Experimental Statistics.
These are not victimless crimes: fraud and scams impose a substantial financial and emotional toll on their victims

Although there are no reliable figures on the full costs of such fraud to the economy, the Centre for Counter Fraud Studies’ Annual Fraud Indicator estimates the cost to individuals to be around £10bn per year – nearly £400 per household. But because a huge proportion is unreported, the true figure is believed to be much higher.¹⁵

Over half of the victims of fraud lose money and about a fifth lose money which isn’t fully reimbursed.¹⁶ In many cases banks reimburse losses in full, but much goes unreported, and reimbursement can depend on the nature of the fraud and the method of payment used (see below). Typical losses are a few hundred pounds,¹⁷ but there is evidence that a small number of people lose very large sums, and are victims over a long period of time. For instance, research by Which? found that 600 victims of scams – who are less likely to be reimbursed than victims of other types of fraud – had collectively lost a staggering £5.6m, with some losing over £200,000.¹⁸ Louise Baxter, of the National Trading Standards Scams Team said to us that her team had discovered many elderly victims who had lost thousands of pounds over decades.

As well as a financial cost, these crimes also leave a harmful legacy for victims’ mental and physical wellbeing. Many of the newer scams hinge on gaining a victim’s trust, or entering into a relationship with them – a process sometimes referred to as ‘grooming’ – with a view to persuading them to transfer money. They then use manipulative techniques such as flattery or making victims feel indebted, in order to pressure victims into making the wrong decisions.¹⁹ As Neil Masters, from Victim Support, told us:

“By its nature, it’s a cruel offence – you are tricking someone.”

One particularly cruel scam is romance fraud, where the target believes they have begun a relationship with the person who is in fact attempting to defraud them. Once the target has fallen for the scammer, they then ask for money, often many times, and over a period of years. When these scams end the victim is left not only poorer but often devastated emotionally. In our interview with Glenn Wicks, deputy chief investigator at the Department for Business, Energy and Industrial Strategy, he told us that, on average, victims of romance fraud lose £10,000.

According to a 2013 report by the Sentencing Council, victims report experiencing panic, anger, fear, stress, anxiety and shame.²⁰ In one study by National Trading Standards a quarter of victims said the crime had affected their health and a similar number said it had made them feel down, or depressed.²¹ Louise Baxter told us that the loss of money and deteriorating health can then make it more likely that older victims enter social care – creating an additional cost for local authorities.

A notable feature is that victims often blame themselves. A NatWest/YouGov research found that nine per cent of online fraud victims felt embarrassed and the same number blamed themselves. Some victims don’t tell neighbours or friends due to the shame they feel, while others withdraw from some social relationships. When people felt the police did not investigate, or take the matter seriously, these negative feelings were exacerbated. The combination of self-blame, perceived low importance of the crime, and low likelihood that it would be investigated, were cited as reasons why many people did not report the crime.²²

---

¹⁷. Ibid.
¹⁸. Which? Briefing on Bank Transfer Scams, provided by Jamie Thunder.
This rise has been driven by changes in technology and consumer behaviour, thus disproportionately affecting the young digital natives

The rise of fraud and scams is strongly connected with the rise in internet usage. 90 per cent of UK households are now online, and four out of five adults now have a smartphone, with more than half now connected to 4G. Nearly two-thirds of people now use internet banking, up from just 30 per cent a decade ago.

Figure 11:

Source: ONS, data for sending/receiving emails in (2011 is missing).

As well as internet banking, new forms of electronic payment are becoming more prevalent. There are now over 100 million contactless cards in the UK, a 20 per cent increase on the year, while PayPal claims to have over 20 million UK users.

Our use of the internet and new forms of digital technology has opened-up a huge range of new opportunities for communication with others – something that is beneficial in countless ways. But it has also made it much easier for fraudsters to contact us. As the cost of emails, texts or phone calls has fallen, sending millions of fraudulent messages to people (often through a simple computer programme or through call centres located in distant parts of the world) can be profitable even if just a tiny fraction of the recipients are fooled. As Chris Felton of the NFIB told us:

“Certainly, the internet has shifted everything. Now we have got crimes like online dating fraud for instance. Ten years ago that would not have existed because people just did not interact that way.”

The increasing use of smartphones and tablets may also be making us less secure. This is partly because consumers are not always willing to use the security measures that are available. Talal Rajab, of TechUK, told us:

“We talk to manufacturers for example, who have security features built into their products, but the end user doesn’t switch them on, because it might slow it down, or it means they have to update it every three months and change passwords.”
Meanwhile, incautious behaviour, particularly among the young, is putting them at risk of fraud. We might expect digital natives to be the most competent users of technology, but in fact confidence can easily slip into foolhardiness. According to NatWest/YouGov research, over 80 per cent of 18-24 year olds are willing to share their email address online with their friends, and as many as 29 per cent are willing to share their mother's maiden name (a commonly used security question). This contrasts with just 60 per cent of over-55s willing to share their email address, and only 12 per cent willing to share their mother's maiden name.

With digital natives much more likely to use smartphones and tablets for online banking and shopping, the fact that users are much less likely to install security software on these devices than they are on laptops and PCs may also be contributing to this group's vulnerability. The research also found that 86 per cent said they would install it on a laptop/PC, only 57 per cent said they would on a tablet, and just 50 per cent on a mobile phone. Partly, this might reflect myths about how secure phones are compared with PCs. Talal Rajab, of TechUK:

“There was this common misconception that just because an operating system is closed source, it is secure. So, there was this idea that closed source operating systems like Apple cannot be hacked.”

The proliferation of passwords and pins for different accounts is also causing trouble. Only 59 per cent of people use multiple passwords and most people save passwords to their browsers, increasing their security risk.

Most importantly, consumers are still too trusting of emails and messages they received. As Chris Felton, of NFIB put it to us:

“The public perception of risk has not yet caught up with reality. People still think that if they get an email with Netflix on it, then it’s from Netflix.”

Tony Neate, of Get Safe Online, agrees:

“People only think about security when something happens to them or a close friends or family. Getting people to realise that it can happen to them and what can be lost – people tend to be blasé about it.”

27. NatWest/YouGov research.
...while the landscape of fraud is complex, constantly changing, and increasingly international in character

Scams and frauds are ancient. But technological changes such as the rise of the internet, use of credit and debit cards, and online purchases and banking, has enabled new complex forms to emerge and proliferate. As Jim Gee, of the Centre for Counter Fraud Studies, told us:

“The environment of scams and frauds is constantly mutating and changing, like a virus.”

FFA UK attribute much of the recent rise in fraud to the growth in “impersonation and deception scams as well as sophisticated online attacks such as malware and data breaches.”

They report that card not present (CNP) fraud, where stolen bank details are used to make purchases, often online, (but without physical possession of the card) now account for 70 per cent of bank fraud losses. The losses from such fraud increased 20 per cent in just one year. E-commerce fraud now accounts for 50 per cent of all card fraud, and 71 per cent of remote purchase fraud.

Most people are already familiar with ‘phishing’ – in which the target is contacted via an email that appears to be from a recognised company or bank, attempting to trick them into entering their login details and password into a fake site with a view to using these to steal money. To phishing we can now add SMiShing (a similar process, via SMS), and vishing (through phone calls). According to NatWest-commissioned survey data, 60 per cent of those concerned about online fraud identified phishing, SMiShing and vishing as their main worry.

Another common crime is the ‘advanced fee’ scam where an individual is contacted by a fraudster, often by email, requesting a small upfront payment, on the promise of receiving a large sum of money at a later date. While this originates from many different countries, it is often referred to as the ‘Nigerian scam’, as one prominent story told by fraudsters involved a supposed Nigerian government official offering the target a share of money which is being illegally transferred out of the country.

As well as these, there has recently been an explosion in new, more esoteric frauds and scams, particularly those connected with identity theft (see box 3). New online platforms, including social media and dating sites, are particular targets for fraudsters to gather personal details, gain the trust of potential victims before requesting transfers, or to recruit ‘money mules’. E-commerce sites such as Ebay have also been used to defraud people by offering non-existent products. In one instance, Russian gangs were flying money mules into the UK every day to open bank accounts, which were then used to deposit the proceeds of scams.

One of the difficulties is that these newer frauds can be initiated by a small number of people, but targeted at thousands or even millions. Carl Miller of Demos explained:

“The problem with fraud and more financially motivated crime, is that a small group of actors can do it at scale. A small group in Russia can defraud millions of people. They’re doing it in an automated way…they’re scanning every device that is vulnerable, and trying to inject malware where possible. With ransomware you can just as easily target ten thousand computers as one computer.”

Another problem is that these crimes are often perpetrated by criminal gangs from anywhere in the world. For instance, as Chris Felton of NFIB told us, a large proportion of online shopping fraud is perpetrated by Romanian gangs, computer software fraud is mostly done from India, while mandate and CEO fraud are often organised from West Africa. This means that the ability of UK police to identify the perpetrators and bring them to justice is limited – such investigations are inevitably

---

29. Ibid.
30. Ibid. Remote purchase, or “card not present” fraud is when fraud occurs without the criminal having the physical credit or debit card, but has the relevant details to carry out an online or telephone transaction.
“expensive, time-consuming and slow”. Furthermore, they can only proceed with the cooperation of the authorities in other countries – this means that those that involve countries with whom there is little cooperation, eg Russia, can be hard to progress. Carl Miller, of Demos:

“If you are in Russia and you defraud someone in the UK, your chance of being caught by law enforcement in the UK is practically nil.”

The scale, constantly changing nature, and international character, of many of these frauds is a huge problem both for consumers and law enforcement agencies. For consumers, the challenge is to continue their lives online without falling foul of the ingenious and ever-changing litany of tricks invented by fraudsters. For the law enforcement agencies, the difficulty is to find the originators, who may be located almost anywhere in the world and use sophisticated technology to obscure their trails.

The situation is exacerbated by a growing problem of cyber attacks and data thefts. Official data on the extent of data breaches has been lacking because companies have generally not been under any legal obligation to report such breaches, when they occur. However survey data suggests that nearly half of all UK businesses experienced at least one cyber security breach or attack in the last 12 months. This rate rises to 68 per cent for large firms. As Glenn Wicks put it:

“Companies are wide open to fraud if they have not been done before and once they are done, they start to block the doors after the horses have bolted.”

Only last month, Equifax, the US credit-scoring firm, lost the personal details of 143 million people, including hundreds of thousands of credit card details.

Once this data has been stolen, as Simon Dukes told us, it can then be ‘warehoused’ and sold on to other criminal gangs, at a price. According to Jim Gee, the data can then be used either to target individuals with certain scams, or it might be sufficient for fraudsters to directly hack into bank accounts and carry out fraudulent transactions.


Box 3: Just a few of the more recent frauds and scams (iv, v, vi, vii, viii, ix)

**Money mules**: Schoolchildren and students are often targeted by fraudsters to set up and give access to their bank account details. These accounts are then used to transfer funds from money laundering, and also to hold money acquired through other scams.

**Copycat (fake) websites**: These are fraudulent websites which replicate a commonly used official or company site, e.g., that of the DVLA, McAfee, EHIC cards. Such websites are sometimes engineered to appear high on search rankings and look very convincing. Some recent cases have targeted students through fake university or Student Loans Company websites requesting updated personal information and bank account details to transfer bursary or prize funds.

**Dating site scams**: Scammers contact people through dating sites to gain their trust and affection. They are then asked for money or may be blackmailed after sharing revealing photos. With the rise of apps such as Tinder, this has become a concern particularly for the younger who are the predominant users of such services.

**Fake news scams**: Clickbait news stories which, after the user clicks the link tell you that you have a virus and ask you to download some software. This software might then lock your computer, or steal your banking details.

**Tech support (vishing) scams**: Victims are contacted by phone from someone who tells them their computer has been infected with a virus or ransomware. They persuade the victim to give them remote access to the computer, which then leads to personal or banking details being stolen. A recent scam involved people claiming to be from Microsoft.

**Ransomware**: Malicious software that takes control of your computer and blocks access to your data unless you pay a ransom or give personal data. This year ransomware called WannaCry and Petya have affected UK households.

**Investment scams**: Fraudsters trick people into investing in wine, gold or other esoteric assets, with the promise of big returns. In a recent example UK pensioners were tricked into investing money into an overseas binary trading platform, from which they couldn’t then retrieve their money.

**Delivery scams**: A fake Royal Mail “You were out” card is left with victims who are then asked to ring a telephone number. But the call costs £45.

---

iv. This is Money: Fraudsters target students as young as eleven at school gates to make them mules in bank account scams, Sept 17, http://www.thisismoney.co.uk/money/beatthescammers/article-4886796/Students-young-11-targeted-a.html


The government has started to respond, but there is a lack of clear accountability and multiple organisations with overlapping responsibilities

In some respects, the UK government has been ahead of many other countries in its response to the growing threat from online fraud. It has published three cyber security strategies since 2009 (now a requirement for all EU member states), and has run an online safety campaign – Get Safe Online – since 2005.

Following the 2006 National Fraud Review, which first recognised the huge under-reporting of fraud, the government set up the National Fraud Authority (NFA) and Action Fraud, to provide a central focus for fraud prevention and reporting. At the same time the National Fraud Intelligence Bureau (NFIB) was created within the City of London Police to collect data, gather intelligence and focus resources on fraud in the UK.

However, in 2014, under the home secretary Theresa May, the NFA was closed and its functions, together with Action Fraud were transferred to the City of London police. Many of those we spoke to said that with hindsight, this had proved unwise. Mark Button, of the University of Portsmouth:

“The NFA was the one organisation with a specific focus on fraud and they were abolished at the very time when the problem was exploding! The NFI (National Fraud Indicator) was also abolished, particularly because the figures were so huge it was embarrassing for the government.”

There are also concerns about the way in which responsibilities for fraud reduction cut across multiple government departments. Louise Baxter told us:

“[The Department for Digital, Culture, Media and Sport] is responsible for nuisance calls and data sharing, Home Office for fraud; Department of Business, Innovation and Skills for mass-marketing fraud; and councils have a duty to protect people from financial abuse. It’s a confusing picture.”

An audit of the different organisations involved in fraud detection and prevention reveals a huge number, with many overlapping responsibilities (see box 4).
**Box 4: Too many cooks? The organisations involved in fraud detection, prevention, and prosecution in the UK**

**Action Fraud:** Run by a private company, their job is to be the national centre of reporting of fraud and cyber crime. They sit alongside the NFIB as part of the City of London police. They pass crimes to the NFIB who use it to identify patterns and then, if there's sufficient evidence, refer crimes to the local police forces for investigation.

**Joint Fraud Taskforce:** Set up by the government but with voluntary participation, this brings together representatives of banks, the criminal justice system, and charities to identify actions they can take to reduce fraud.

**National Fraud Intelligence Bureau (NFIB):** Now part of the City of London police, their job is to gather and analyse intelligence relating to fraud. They use this to identify patterns and perpetrators.

**National Cyber Security Centre:** Part of GCHQ, their role is to try to prevent cyber attacks and make it safer to live and do business online.

**Payment Systems Regulator (PSR):** A subsidiary of the Financial Conduct Authority, they act as the economic regulator of payments systems in the UK, with the objectives of promoting competition and protecting businesses and consumers.

**Get Safe Online:** A public-private partnership aiming to provide clear and reliable advice for consumers and businesses on how to prevent fraud and prevent harms that could result from using the internet.

**Cifas:** A not-for-profit organisation that encourages organisations to share information on fraud and financial crime. They now have 400 members who share information with a view to identifying perpetrators and preventing fraud.

**Financial Fraud Action (FFA) UK:** Part of UK Finance, this organisation aims to act on behalf of the payments industry to reduce financial fraud. It oversees the Financial Fraud Bureau (FFB) which organises information-sharing and dissemination. The FFA, in partnership with the Metropolitan police and the City of London Police, also have a law enforcement unit – the Dedicated Card and Payment Crime Unit (DCPCU).

**National Crime Agency (NCA):** Their role is to protect the public from serious and organised crime. One of its units is the Economic Crime Command who oversee and tackle economic and financial crime.

**Serious Fraud Office (SFO):** A government agency that investigates and prosecutes complex and serious fraud, bribery and corruption.

**Police and Crime Commissioners:** Replacing police authorities, they are responsible for setting local priorities and allocating funding for policing in their area. They also appoint and dismiss chief constables who run the local police forces.

**National Trading Standards e-Crime Unit (NTSeCT):** A new national team set up to protect consumers and businesses against online crime and fraud. Sponsored by the Department for Business, Innovation and Skills, and the National Trading Standards Board, it combines teams of crime analysts and internet investigators to gather intelligence and investigate offences.

**Financial Conduct Authority (FCA):** The principal regulator of the financial services industry, part of their responsibility is to reduce financial crime, which includes frauds and scams.
In 2016, the Joint Fraud Taskforce was created to spearhead an aggressive new approach to tackling fraud. For the first time, banks, the police and government are working together to prevent and disrupt fraud, developing a cross-industry strategic plan. There have also been several government and industry-led campaigns aimed at reducing fraud. The National Audit Office highlighted thirteen different campaigns, of which the two most notable are:

- **Take Five** (https://takefive-stopfraud.org.uk): a campaign led by FFA UK, Cifas, all UK banks and the City of London Police, which aims to highlight some simple steps consumers can take to reduce the risk of fraud.

- **Cyber Aware** (https://www.cyberaware.gov.uk): a government-led campaign, initiated by the Home Office and funded by the Cabinet Office, to help consumers and businesses be safer from cyber criminals.

Another key awareness programme is Friends Against Scams, run by the National Trading Standards Scams Team, which won the 2016 Government Counter Fraud Award for Excellence in Fraud Awareness. Since the team’s creation in 2012, its support and referral system has saved UK consumers over £50m. In the latest programme, the NTS Scams Team have partnered with NatWest, the campaign group Think Jessica, the Chartered Trading Standards Institute, Bournemouth University and the Older People’s Commissioner for Wales. It targets hard-to-reach communities, relying on volunteer ‘Friends against Scams’ who are asked to share their knowledge about scams by making a pledge, such as telling five people about the initiative and taking precautions, sharing information on social media, displaying a poster or helping someone who has been the victim of a scam.

While such awareness-raising efforts are clearly an important part of the fight against fraud, some of the people we have spoken to thought that they can only have a limited impact on the problem in the short term. Jamie Thunder, of Which?, told us that awareness campaigns are not likely to stop the majority of frauds, for two main reasons:

> “First, scammers are a kind of businessman, they are always going to adapt, so consumers will have to be one step ahead all the time. So, it follows that we would need a constant stream of updated campaigns. And second, consumers have to see the campaign, and be reminded of at the right time, and change their behaviour. This is a very high hurdle.”
And the criminal justice system still hasn’t adapted to these new realities

The police force has, in recent years, faced significant cuts in funding, with overall police numbers falling 19 per cent since their peak in 2010.\footnote{37} For some, these cuts reflect the faulty view that crime has been falling, when in fact it was simply moving online. Carl Miller, of Demos:

“The really massive problem is that this apparent drop of crime has been used as a political argument for reducing the amount of funding the police receive. So right at the moment when cybercrime began to increase, we thought crime was falling.”

But even before this, the resources dedicated to fraud were limited. Between the 1980s and 2006, the number of fraud squad officers fell from 588 to an estimated 416. Miller also argues that the structure of the police, separated into 43 local forces, is not suitable for tackling cyber crime and fraud which typically crosses regional and national borders:

“We’ve split the UK into 43 small territorial groupings that are primarily dedicated to local policing, which is the opposite of what you need if you want to try to police the internet effectively.”

At the same time, the training of police officers is still not geared towards online crime. The main course on cyber crime began in February 2014, but the Home Office stopped its funding in April 2015.\footnote{39} There is still considerable evidence that the police don’t investigate crimes properly, and sometimes don’t understand how to treat the victims of these crimes.\footnote{40} Mark Button, of the University of Portsmouth told us:

“Many police chiefs are still focussed on traditional crime. Lots of police officers often struggle with modern technology and don’t understand the new problems it creates.”

A 2015 study by HM Inspectorate of Constabulary found multiple failings in the handling of reporting. According to that report, neither the police not public understand the role of Action Fraud.\footnote{39} People are still reporting fraud to local police, while the police are wrongly referring them to Action Fraud. In our interview with Glenn Wicks he told us:

“Police offers have been encouraging people to report to Action Fraud, even when they should be dealing with fraud themselves.”

Cases reported to Action Fraud take at least 30 days to allocate to an investigator – by which point the opportunity to stop or recover funds has already passed.\footnote{42} It seems that some local police forces wrongly believe Action Fraud has assumed all responsibilities for fraud. When cases are referred to them from the NFIB they are often not followed-up or simply ignored due to cost concerns.\footnote{43}

The idea that the police no longer believe they have responsibility for fraud is backed-up by the number of staff allocated to that area. Although fraud now accounts for about 30 per cent of all crimes,\footnote{44} according to one estimate the proportion of officers working on fraud is just 0.27 per cent.\footnote{45} Katy Worobec of UK Finance told us:

“There is a disconnect between the Home Office, who do view economic crime as a major priority, and the local forces who, by and large, do not.”

Glenn Wicks agrees:

“Fraud won’t be taken seriously by the police… it is not a key policing objective to investigate fraud.”
Even when frauds are considered suitable for investigation and prosecution, it rarely results in prosecution. Statistics gleaned from Freedom of Information requests by the BBC 5 Live team indicate that if you reported a fraud in 2015-16 the odds that it would be referred to local police for investigation were just one in 10, the odds of it ending in court were one in 70, and the odds of a judicial sentence were about one in 350.⁴⁶ (And these numbers excluded the massive number of frauds that go unreported.) The problem may well have worsened since as fraud prosecutions have been in decline (see figure 12).

![Figure 12: Number of people sentenced for fraud offences](image-url)

**Source:** ONS, data for sending/receiving emails in (2011 is missing).

---

⁴⁶ Analysis of excel spreadsheet shared with Policy Network by Professor Mark Button, University of Portsmouth.
Meanwhile, banks have responded, but they are hampered by existing technology, regulations and limited coordination

To combat fraud banks and card issuers have taken a number of steps together through Financial Fraud Action, which co-ordinates the industry’s efforts to tackle fraud within UK Finance. The industry body reports that £750m of fraud was prevented in the first half of 2017, representing two thirds of attempted fraud.⁴⁷ Recent measures that may have contributed include the Take Five campaign (see above), the data breach protocol, which outlines how breached companies should inform banks in the most efficient way, and the Banking Protocol.⁴⁸

To combat fraud conducted beyond the reaches of their staff, some banks have also introduced two factor authentication systems, for example where you insert your card into a reader which then gives you a one-time passcode. However, take-up is not yet universal and there is no common industry standard.⁴⁹ Once final technical standards are agreed, the Payment Services Directive (PSD2) will require all banks to adopt Strong Customer Authentication.

This means that banks will ask customers to use at least two security measures from a selection of something they know (eg a password or pin), something they possess (eg a card reader or their mobile phone) or something personal (eg a fingerprint, iris scan or face recognition) to authorise payments.⁵⁰ Technical standards are currently being drafted which are likely to become effective in the second half of 2019, and are expected to bring some basic standardisation to payment authorisations, although banks may still adopt slightly differing methods.

Neil Masters told us that when making a bank transfer soon you will be able to use the sort code and account number to check the name of the account holder. This move by the banking sector will help reduce scams such as invoice re-direct, where businesses are tricked into making a payment into an account controlled by a fraudster. While coordination has improved in recent years through UK Finance and now the Joint Fraud Taskforce, gaps remain. For example, as Jamie Thunder of Which? told us, technological innovations are not coordinated at an industry level. If one bank improves its security, the criminals may just move to other banks that are more vulnerable, or shift the focus to more vulnerable consumers.

“If there is a weak link in the industry, scammers will just move there. This also explains why there has been a shift from hacking towards scams. Banks’ online protocols are pretty robust, so scammers have moved to the “weakest link” – the consumer. Now it is easier to trick someone to make a transaction, than to hack a bank account.”

---

Box 5: The Banking Protocol (x)

The protocol is a partnership between banks, law enforcement and trading standards officials to work together to identify and stop scams, arrest perpetrators and support victims. If cashiers suspect a scam is in progress or a customer is acting under duress, they can call 999 and receive a guaranteed response from the police. Police will then attend the bank, arrest perpetrators, while trading standards officials can refer them to victim support services. By August 2017, 899 calls had been made, preventing the loss of £6.1m and leading to 65 arrests. The initiative is now being rolled out across the UK. The initiative won the Outstanding Collaboration award at the recent Annual Government Counter Fraud Awards.

---

x. Interview and emails with Katy Worobec, UK Finance.
⁴⁹. Financial Fraud Action: Protect Your Online/ Mobile Banking, https://www.financialfraudaction.org.uk/consumer/advice/protect-your-online-mobile-banking/
Banks are working with law enforcement authorities to track and disrupt the flow of fraudulent funds. However, in practice this is very difficult because, as Katy Worobec told us, the fraudsters often use multiple, linked accounts, which may not present any indicators of fraud (because account holders are either recruited post account opening or specifically selected to avoid detection). This is why Which? is calling for Payment Service Operators (PSOs) – eg Bacs and Faster Payments – to play a bigger role in identifying and flagging suspicious accounts and activity.\(^1\) The PSR has recently highlighted an initiative led by the Payments Strategy Forum to develop industry-wide rules that would allow for a network-wide analysis of transaction data to help this identification process.\(^2\) However, some industry experts believe that to successfully monitor and disrupt these financial flows, legislative change may be required, for example to ensure victims have losses from fraudulent payments reimbursed.

Many would like the banks to do more to prevent scams by delaying or stopping suspicious transactions from occurring. However, as Katy Worobec told us, banks are under a legal obligation to carry out transactions a customer has authorised, and the Faster Payments Service also makes delaying payments difficult.

… and there is confusion about where the responsibility to prevent APP scams lie

There are growing voices calling for banks to take more responsibility for frauds. There is particular controversy surrounding the problem of Authorised Push Payment (APP) scams – where there has been no unauthorised access of an account, but someone has been tricked into transferring money to fraudsters. This could happen eg through romance or advanced fee scams.

At the moment a victim’s chances of being reimbursed after a fraud or scam differ hugely depending on the mode of payment used. Banks typically have to reimburse customers for fraudulent losses on credit and debit card transactions (barring gross negligence or the victim engaging in fraudulent activity). But this is not the case for bank transfers, where victims are usually only reimbursed if the payment was unauthorised. If a person is tricked by scammers into sending money to them via bank transfer, particularly if it is through the Faster Payments System, there is little chance the funds will be reimbursed when the scam is identified, because the payment was authorised by the customer.\(^3\)

This prompted consumer organisation Which? to make a super-complaint to the Payment Systems Regulator, calling for the banks to have greater liability over APP scams involving a bank transfer. In Which’s preferred option, banks would be made liable for reimbursing consumers that were victims of a scam (barring the victim acting fraudulently or with gross negligence), effectively extending the protection currently available in relation to unauthorised payments.\(^4\) The PSR issued its response, agreeing more work was needed, but rejecting the call for widescale reform, partly because of the danger of moral hazard – that if banks assume liability, it will encourage more risky behaviour from consumers.

In November 2017, the PSR launched a consultation on a ‘contingent reimbursement model’. Under this regime, banks would agree to meet certain standards to help prevent APP scams, and would have to reimburse the victim if they failed to meet those standards, provided the victim took the requisite level of care. The PSR provides several possible options what should happen if both parties (the bank and consumer) took the appropriate steps but a scam still took place, with options ranging from Which?’s preferred option (reimbursement by the bank), reimbursement from a central fund to which all banks contribute, to no reimbursement.\(^5\)
While there have been promising new technological innovations in some areas, the response of the technology and social media giants has been muted

There have been significant recent developments in both new card technology and fraud prevention for retailers. Paul Naldrett of Idemia (formerly OT-Morpho) told us how his company is developing promising new solutions to bank card fraud, such as digital display cards, fingerprint cards, and working with government to spread the use of the UK government’s Verify programme into industry (see Recommendation 5 for more on this). In addition, ClearSale, a Florida-based company, has developed a powerful new platform, combining both artificial intelligence and manual review which help retailers prevent fraud. Bruno Farinelli, of ClearSale, told us that this has enabled their customers to reduce fraudulent transactions by 90 per cent, while reducing the number of false positives (legitimate transactions that are declined) close to zero.

The response of technology companies such as Google and Facebook is based primarily on the idea that it is the responsibility of consumers to identify and avoid scams. Google uses two-step verification on its email accounts, SSL encryption and software which identifies and blocks spam before it reaches your inbox; they claim that less than 1 per cent of spam arrives in someone’s inbox.²⁶ They also say they identify and flag 10,000 unsafe sites every day. Facebook also has two-factor authentication (although users must opt-in). However, the bulk of its Account Security section (buried in the website) seems devoted to things users need to do to stay safe;²⁷ while users are encouraged to report hacked or impersonation accounts.

But these companies are far from safe. ‘Gooligan’ hackers recently broke into 1.3 million Android phones, bypassing two-stage authentication and enabling them to hack Gmail accounts, and access personal data. Victims were forced to download apps and submit positive reviews.²⁸ Google Play has been found to have apps which contain malware.²⁹ It has also been plagued by millions of fake ads, which direct users to fraudulent goods or websites or download malware.³⁰

Increasingly fraudsters are using social media sites such as Facebook to look for personal details which could help them commit fraud, and to recruit ‘money mules’ to move around money gained from fraudulent activity.³¹³² Computer viruses are being used to target social media sites with a view to infecting the users’ computer, as in “Koobface”.³³

Delia Rickard, deputy chair of the Australian Competition and Consumer Commission, told us that social media companies are not doing enough to tackle scams:

“They’re making the right noises. Certainly, we can refer individual instances of scamming for them to take action. However, we would be very keen to see them do more systematically to really identify scammers on their site, and get rid of them. We think there’s more they can do.”

57. Facebook: Security Tips: Here are 6 things you can do to help keep your account safe, https://www.facebook.com/help/keeping-your-account-secure/ctx
data
4. Recommendations

1. **Government should ensure the next generation of digital natives know how to stay safe online, stepping up online safety education and making all teenagers complete a short, online course in cyber security, fraud and scams before they leave school**

This report highlights the myth that fraud is experienced disproportionately by older people. They remain the target of fraudsters, and when suffering from ill health or social isolation, can be particularly vulnerable. Age UK has done a good job of highlighting the problem, and the National Trading Standards Scams Team has developed successful strategies to disrupt many frauds experienced by these groups.

However, we have seen that in fact younger people are now disproportionately the targets of fraud. Cifas are currently piloting fraud awareness classes in fourteen schools. Meanwhile, the National Cyber Security Centre are running CyberFirst courses which educate 11-17 year olds in cyber security. Similarly, NatWest runs the MoneySense programme for 5-18 year olds, providing learning materials (which incorporate fraud modules) for parents and teachers as well as workshops assisted by bank employee-volunteers.

But we need to reach more young people. The aim should be that all schoolchildren complete a short course on fraud, scams and cyber security by the age of 16. Government, working with the Joint Fraud Taskforce, should develop and fund a nationwide course programme that meets this objective. This would ensure all young people on the cusp of financial independence are better equipped with skills to stay safe and keep their money secure.

As well as encouraging long-term behaviour change, students should be encouraged to make vital security changes there and then. While learning about online safety, they should be prompted, for example, to review privacy settings on social media and download protection software for online banking, as well as encouraging participation in the Friends Against Scams programme. To prevent this taking up scarce time in the curriculum (eg PSHE), the best approach would be to develop a short online course which students complete outside school. In turn, this would prompt discussions around online security to take place in the home, spreading awareness within families.

While late adolescence is an important moment to teach practical skills and prompt individuals to make changes as they gain financial independence, interventions can and should also be made much earlier. After all, 12-15 year olds now spend over 20 hours a week online. We welcome the children’s commissioner’s recent calls for a step change in how children are prepared for digital life, including a compulsory digital citizenship programme from ages 4-14, the introduction of simplified terms and conditions for digital services offered to children, and a new children’s digital ombudsman to mediate between under-18s and social media companies. New programmes being set up should also draw on the work of the Financial Capability Evidence Hub, which is bringing together evidence from pilots, programmes and policies across Britain to help build up the evidence base for effective educational interventions in this space.

2. **The banking system needs an industry-wide initiative to tackle CNP fraud by upgrading card technology**

The introduction of chip and pin cards over a decade ago had a significant impact on fraud, making it much harder for criminals to steal cards, or make transactions by faking signatures. But the benefits
of the system have now worn off, and CNP fraud is now a massive and growing problem – it accounts for around two thirds of bank fraud.

A new technology is needed to make bank cards fit for the next generation of card-users. The most plausible current candidate is the digital display card (see box 6). It is estimated that they could cut CNP fraud by up to 80 per cent. Another part of their appeal is that, unlike chip and pin, it would not require retailers or electronic merchants to change their payment systems. They are already being experimented with by Mastercard and Visa. However, this development is currently being held back by cost (these cards cost four to seven times more than a normal card).

**Box 6: Digital display cards**

Digital display cards are like normal bank cards, but which include extra technology that prevents fraudulent use, even if the card details have been compromised.

There are two main types:

**Dynamic CVV2 card:** This is a card that has a digital mini-screen on the back with a security code that automatically changes according to an algorithm every hour. So even if a fraudster had the security code, it would become obsolete before they could commit much fraud. The downside is that consumers would need to have their card physically present in order to authorise transactions.

**All-in-one digital display card:** This is a card which includes a digital display and small keypad, allowing users to enter authentication codes without the need for an extra card reader. This also allows the security code to change, but additionally makes electronic payments more secure, satisfying the idea of strong authentication.

An alternative to digital display cards is cards with integrated fingerprint readers. These allow the user to authorise payments through a fingerprint scanner embedded in the card itself. Paul Naldrett of Idemia (formerly OT-Morpho) told us that they are developing a version of this called the F-card. These are more technically challenging than digital display cards because they require a secure way of initially verifying the fingerprint. Depending on how they are implemented there may also be a risk that the fingerprint data is stolen by hackers. However, they are growing in popularity and are now being used in parts of Latin America, where the fingerprint data is stored in an individual’s card, rather than held centrally.

An even more radical idea is to change the default card setting from ‘on’ to ‘off’. At the moment bank cards can always be used for transactions, anywhere in the world, provided the bank details, pin and security code are entered correctly. That’s convenient but it means that if those details fall into the wrong hands there is little to stop fraud from happening. Some banks already allow customers to switch their cards off temporarily if they have been misplaced or lost. But what if that idea was taken a step further so that the default setting for cards was ‘off’ and you had to turn them on using an app on your phone? And the payment could be authorised by using your phone’s GPS to check that you are in the same place as your card? An additional measure would be to allow card holders to set their own transaction limits and restrict purchases to only certain countries. Then CNP fraud

---


72. NatWest: Interview with Paul Naldrett of Idemia (OT-Morpho).


would be much more difficult. That’s the idea behind Neo Africa’s Secure Card, a new concept being
developed by a South African company.73

So, government should work with the banking sector to explore, develop, and finance, a new
industry-wide card technology. Once an appropriate solution has been identified, the government
should set a deadline by which all cards need to be converted to this standard.

3. Government should work with the Joint Fraud Taskforce to design and re-introduce
   a National Fraud Indicator and an ambitious target for fraud reduction – a 25 per
cent reduction by 2025

When the NFA was abolished, so too went the National Fraud Indicator, which provided an
assessment of overall financial losses to fraud across the UK. This means that there is currently no
official national measure of fraud which can provide the focus for government action. Outside
government the Annual Fraud Indicator74 is still produced each year; unlike other measures of fraud
which rely on detection (and therefore tend to under-report fraud) it uses a sophisticated sampling
methodology to provide accurate estimates of the losses to fraud.

If fraud is to be taken more seriously, we urgently need a new official measure of the full extent of
fraud, particularly of the prevalence and losses due to financial fraud, including scams. The Joint
Fraud Taskforce, in conjunction with the Home Office, is currently developing a set of targets for
fraud reduction. So those conversations are the ideal springboard for the development of a new
national target. The Office for National Statistics’ experimental statistics are a good start in reflecting
the prevalence of fraud – but the Annual Fraud Indicator is a more robust measure of the extent of
financial losses. The ideal measurement would include both, in some form.

So, the government should, by working with the Joint Fraud Taskforce and other interested parties,
consult on the creation of a small number of high-level indicators of fraud which are then tracked by
the Office for National Statistics each year and become national statistics. By setting an ambitious
target – eg that fraud be cut by 25 per cent by 2025 – it would send a clear signal of the determination
described by the criminal justice system.

4. Government should bring together existing resources into a new national Economic
   Crime Agency, with powers to investigate, disrupt and prosecute for frauds and scams

Government deserves credit for the initial creation of Action Fraud and the NFIB, organisations
that are doing good work under very difficult conditions. But the current panoply of organisations
involved in fraud detection, prevention and prosecution cannot be optimal. The Joint Fraud
Taskforce has an important role to play co-ordinating from a policy perspective, but there are too
many organisations, with often overlapping responsibilities: this makes for weak accountability,
multiple overlapping initiatives, and difficulties in coordinating actions. Even more seriously, since
the abolition of the NFA, there has not been a single national centre for the detection, investigation
and disruption of organised, low value, high volume fraud.

A new organisational ecosystem is needed, with a single organisation at the centre co-ordinating
all anti-fraud and cyber crime initiatives, with clear lines of reporting and accountability. This
could be called the Economic Crime Agency, and would bring together the NFIB, Action Fraud,
and the Economic Crime Command of the NCA, together with some resources and responsibilities
from organisations such as the National Cyber Security Centre. It should also have the power to
investigate, disrupt and prosecute, as experience so far with the referral of crimes by the NFIB to

www.neoafrica.com/neo-secure/
74. Crowe Clark Whitehill: The
Financial Cost of Fraud 2017.
The latest data from around the
croweclarkwhitehill.co.uk/wp-
content/uploads/sites/2/2017/02/
crowe-the-financial-cost-of-
fraud-2017.pdf
local police forces has not been a success. Forty-three local police forces are not well equipped to carry out these complex, data-driven cases which cut across jurisdictions.

This Economic Crime Agency would be the key agency spearheading government action against consumer fraud while the Joint Fraud Taskforce would retain an important policy-setting and coordinating role across the public and private sectors.

5. **Local police forces should reallocate resources and staff into economic crime and introduce web constables**

The police service has been under financial and staffing strain for a number of years. And undoubtedly it is under constant pressure to tackle growing threats such as international terrorism, human trafficking and child abuse and exploitation. Theirs is not an easy job, and no one is claiming that there aren’t other equally pressing priorities. But, as this report has argued, the sheer scale and harm caused by fraud makes the lower priority it is still given by local police forces both unfair and inappropriate.

While the investigation and disruption of complex frauds is best undertaken at a national level (see above), there is still a vital role for local police in monitoring and warning the public about these crimes, as well as providing support for victims. One model which could be explored that could help digital natives in particular is the idea of ‘web constables’ – police officers which, instead of patrolling a physical space, monitor cyber space with a view to identifying and preventing cyber crime and fraud.
6. **Fraud investigations could make greater use of social network analysis, which will require better data-sharing across government departments and agencies**

As this report has argued, fraud is now a complex, international crime that typically involves a myriad of transactions moving out of the bank accounts of numerous people, some of whom appear legitimate. That’s what makes it so hard to investigate and prosecute. But new tools such as social network analysis are emerging which can have a powerful impact (see box 8). Greater use of social network analysis, underpinned by data-sharing across government, could be a vital tool in identifying, disrupting fraud, and bringing the perpetrators to justice.

---

**Box 7: Estonian web constables**

Since 2011, Estonia, a pioneer in digital services and security, has employed web constables – police officers who monitor and post mostly on social media sites such as Facebook. They are available for people to report crimes to, as well as offer advice and warn of crime and threats, including scams and frauds. People can report suspected scams or frauds to them and the constables will provide advice, and then refer the case for fraud investigation. They also give about a hundred lessons in schools each year about the internet safety. According to Maarja Punak, one of the major benefits of web constables is that they are not limited to a single police jurisdiction. As she put it:

> “Online fraud cases are not strictly connected to a territory - the criminal can be in one city, the victim in another one and the crime itself can take place in another country.”

> “People nowadays prefer texting to face-to-face interactions and it is easier for them to contact the police through social media.”

The web constables are now a well-known feature of the Estonian criminal justice system, particularly among children and young people. A 2014 survey of Estonians found that 61 per cent were aware of web constables, and almost one in ten of these had approached one. Rates of fraud in Estonia are about a fifth that of the UK, and rates of fraud as a proportion of transactions fell nearly 40 per cent per cent between 2009 and 2013.
7. The telecommunications and social media firms need to work more closely with banks and government organisations to tackle the problem

Phishing and SMiShing are currently the biggest source of fraud. But none of them could take place without email, phone, or SMS services, which are provided by telecommunications and technology companies, not banks. But a consistent theme of our research has been that, by and large, these firms are not working as closely as they could with banks and the police to stop fraud. That needs to change. The Joint Fraud Taskforce should establish a sub-committee, with these companies as members, which works specifically on identifying new measures to tackle phishing, vishing and SMiShing, as well as sim-swap fraud, call-line diverts and SMS takeover attacks.

A key priority should be to ensure that consumers can receive comprehensive call-blockers as a standard option for any landline. Another area of focus should be to encourage social media firms such as Facebook and Twitter to put processes in place to report and remove links to fraud and scam related sites by amending their community guidelines and reporting criteria.

8. The government should review how financial losses that result from APP scams should be allocated between consumers, banks, and telecommunications and technology companies

The current division of responsibility, which almost entirely protects consumers from credit and debit card fraud, but hardly protects them at all from bank transfer fraud is untenable. Some banks may move towards a 'no quibble' policy for their own customers, but an industry-wide standard is required to avoid arbitrariness and unfairness. The current situation also unfairly excludes from liability the telecommunication, technology and social media companies whose services are very likely used to transmit fraudulent messages.

Box 8: Pioneering social network analysis in Belgium (xii, xiii, xiv)

Social network analysis (SNA) is a set of data mining methods emerging in fraud detection. These include identifying and visualising relationships – including transactions and social media connections between given individuals or businesses of concern. It also involves detecting rings of organisations or people, and identifying leaders in fraud networks.

The Belgian government successfully employed SNA to tackle carousel fraud (a complex fraud which involves defrauding the tax authorities of VAT payments). Their fraud detection model involved mapping known fraudulent transactions, flagging suspicious behaviour, then using predictive models to suggest where fraud might occur next. They could then act swiftly to disrupt the frauds and arrest perpetrators. This led to a 90 per cent fall in carousel fraud, saving nearly a billion euros. The model is now being replicated across Europe.

But crucial to making SNA effective is data-sharing across different parts of government, so that the social network analysis can be carried out.
There are arguments for banks assuming more responsibility, including that it would encourage banks to introduce more security measures, and that it protects vulnerable consumers. But equally, as the PSR found in response to Which?’s super complaint, there is a need to avoid the problems of moral hazard, and ensure consumers have good reason to behave responsibly.

9. No loopholes or caveats: all companies should have to report data breaches

Until recently there was no legal obligation on companies to report cyber attacks, or data breaches, with the Information Commissioner’s Office instead relying voluntary reporting. As a result, we are probably only aware of a small proportion of the attacks that have taken place, where it came to the attention of the media or where the company took the decision to go public.

This lack of transparency fostered a culture of secrecy, which allowed companies to conceal the true scale of the problem. This in turn has put consumers at unnecessary risk, because they have, in many cases, not been informed that their data has been lost, and therefore been unable to take pre-emptive actions. It has also meant that the government and criminal justice system has been unable to establish a clear benchmark against which the problem could be monitored.

In 2003, telecommunications companies and ISPs were made subject to mandatory reporting and in May 2018 the EU General Data Protection Regulation (GDPR) will come into force which will force all companies to report data losses. However, this legislation is subject some important caveats which may, in practise, make it less effective. For instance, companies will only have to report data breaches within 72 hours and they don’t have to report it if it is “unlikely to result in a risk to the rights and freedoms of data subjects”75. This puts the onus on companies to decide whether the data breach is a risky one or not. That make the situation unclear, and could lead to under-reporting.

In the short-term, government has indicated that we will retain the GDPR even while we leave the EU. However, in the longer-term Brexit provides an opportunity for the UK to ‘gold-plate’ these reporting requirements by establishing a new universal mandatory reporting standard for data breaches – regardless of perceived magnitude or seriousness – within 24 hours of the breach happening. Such a standard will force data breaches into the public domain, providing a true picture of the problem, and encouraging companies to adopt more secure systems. By going public earlier with data breaches, it would also enable customers to take speedier action to protect themselves.

10. The government should invest more in victim-orientated approaches to disrupt scams through the use of financial intelligence

The identification and prosecution of the perpetrators of these crimes is difficult and costly because they are hard to find and are often abroad. And in any case, their prosecution comes too late for the victims. So, just as important as bringing the perpetrators to justice is disrupting crimes that are in progress.

In Australia, the Competition and Consumer Commission runs a Scam Disruption Project modelled on a previous successful scheme, Project Sunbird based in Western Australia.76 Potential victims are identified using financial intelligence and sent a letter explaining that they might be victims, encouraging them to stop sending money, and requesting they make contact with officials. If they continue to send money after a second, more targeted letter, payments can be interrupted, and investigation commenced focusing on both local and overseas suspects. Results have been positive. Of those sent a letter by the ACCC, 74 per cent have stopped sending money within six weeks, with fund transfers to high-risk jurisdictions down by over $1m from 2015 to 2016.

A similar UK-based scheme run by the NTS Scams Team is now yielding good results (see box 9). Government should ensure that this, and the related police initiative Operation Signature, are adequately funded. However current schemes are mostly targeted at elderly people. We need to broaden the scheme to target other demographic groups.

### Box 9: Disrupting scams – National Trading Standards Scams Team

Many victims of scams may not realise that is what is happening. Or if they do, not tell anyone or report it to the authorities. This is particularly likely for older victims who may be more vulnerable due to dementia or social isolation. So, the scams can continue for many years and lead to huge losses of money, while the authorities remain oblivious. One elderly man in Hampshire transferred over £100,000 to scammers. The NTS estimate that such scams are costing people £5-10bn per annum.

Recently the authorities in the UK have developed new initiatives aimed at identifying these people and halting the fraud. What is now the National Trading Standards Scams Team started in East Sussex trading standards, where a pilot was launched in 2012, using ‘suckers lists’ with over 106,000 names. The NTS Scams Team work with local authorities to identify possible victims in their areas, contact them, and intervene to ensure the victimisation doesn’t continue. An evaluation found that the pilot saved at least £56 for every £1 spent as of last year’s annual report. Operation Signature, a similar scheme run by Sussex police, is also delivering good results. However, for this method to work, there needs to be adequate data sharing between banks, telecommunications providers, postal organisations, and the police to develop lists of people who may be at risk. And the teams of investigators need to be properly resourced to be able to reach enough of the potential victims.

11. **Banks should work with the government and regulators to develop an equivalent to the Banking Protocol for electronic transfers**

Banks are under a duty of care to their customers not to facilitate fraud, but at times this can conflict with their strenuous legal duty to carry out transactions where those have been given the consent of the customer.77 This means that it may be difficult for banks to refuse to transfer money even if they believe the customer to be the victim of an ongoing scam. However, the Banking Protocol is a promising new initiative that has allowed cashiers in bank branches to quickly alert the police to possible scams in progress, enabling transfers to be stopped, and arrests be made (see above).

As successful as the Banking Protocol has been, with such a high proportion of transfers now taking place online rather than in-branch, further work is needed. Banks should build on the innovation and spirit of cooperation that helped to create and implement the Banking Protocol, and work with the police and National Trading Standards Scams Team again to develop a new, step-by-step approach for tackling scams involving online bank transfers. Suspicious transactions should be flagged, delayed, and potentially disrupted either by the bank, police or trading standards officials. Banks will need to work with the FCA, PSR and PSOs to identify and overcome any legal or regulatory hurdles which currently hamper this.

---


Interview with Louise Baxter.
12. Banks should encourage – both through innovative design and financial incentives – customers to choose a package of new, more secure, banking services which reduce the scope for APP scams

Although most bank customers will continue to prioritise convenience, rising awareness of the threat of scams and frauds should encourage consumers to seek banking services that make them less vulnerable – particularly given the danger of funds not being reimbursed. Without changing regulations, there is more banks could offer to meet this demand.

For instance, they could offer as an ‘add-on’ to an ordinary current account a service that provides an automatic 24hr delay on payments over a certain amount (say £1,000), geographic restrictions on where money can be paid, and automatic warnings when transfers are being made to a new payee. Or perhaps accounts could have a nominated ‘next of kin’ who is alerted via text when large or suspicious transfers are being made from the account. For vulnerable customers, banks could offer more restrictive accounts with, for example, lower spending limits and delayed payments.

For the vast majority of customers, these should not pose any serious inconvenience, and for many, the prospect of more secure services will be enough to motivate them to take up the offer. However, some customers will need a stronger nudge, and since services will reduce future costs of fraud and scams, banks should also offer financial incentives such as better interest rates or bonus payments, to take them up. There may even be a case for making this package automatic (ie opt-out) for customers that have been previous victims of fraud, or who fall into a vulnerable category. Better data-sharing between the private and public sectors (such as NTS, councils and local health services) would help to identify at-risk groups.

13. Technology and telecommunications companies should make computers and phones more secure, by design

At the moment, if you buy a laptop, you may not have any virus protection included, and if you do, there is nothing to stop it lapsing when the initial free trial has ended. That puts millions of consumers at unnecessary risk from computer viruses, malware and ransomware that could lead to fraud. One idea suggested by more than one of our interviewees is that virus protection should be automatically installed on every desktop, laptop, tablet and phone sold, and that it should also be updated automatically. Consumers would benefit dramatically from the knowledge that their device is secure from the point of purchase, and would have a dramatic impact on the problem of computer misuse and related fraud.
5. Glossary

See box 3 for a list of the most recent frauds and scams and box 4 for the organisations involved in fraud detection, prevention and prosecution in the UK.

**Fraud:** In this paper, we define fraud as any act of deception for the purposes of financial gain. It includes cases where the criminal has gained unauthorised access to a victim’s bank card or account, whether online or offline, as well as scams, where the victim has been tricked into authorising a payment or transfer themselves.

In the Crime Survey of England and Wales, fraud is divided into four categories: Bank and credit account fraud, advance fee fraud, non-investment fraud and other fraud.

**Scam:** A type of fraud where a criminal deceives the victim into authorising a payment or transfer of funds, for example by pretending to be someone they are not and appealing to their emotions (e.g., with romance scams) or the promise of a bigger return at a later date (as with advance-fee scams). Instances where a victim is deceived or blackmailed into giving their bank card or account details to a criminal, that are then used to carry out fraud, may also be referred to as a scam.

**Bank and credit account fraud:** Fraudulent access to bank, building society or credit accounts, or fraudulent use of card details.

**Card not present (CNP) fraud:** Specifically where a criminal gains access to a victim’s bank details (either through hacking, blackmail or deception), and uses those to make purchases without physical possession of the card.

**Identity fraud:** The use of stolen personal details to obtain goods or services by deception. CNP fraud is one method, while others might include setting up a bank account or obtaining a loan, credit cards or state benefits in the victim’s name.

**Non-investment fraud:** The Crime Survey of England and Wales describes this as comprising “cases where the respondent [victim] has generally engaged with the fraudster in some way, usually to make a purchase which is subsequently found to be fraudulent, for example, online shopping, bogus callers, ticketing fraud, phone scams and computer software service fraud”.

Many of these frauds would also be known as a ‘goods not received’ scam.

**Investment fraud/scam:** Refers to financial investments that turn out not to exist, or were otherwise made under false pretences.

**Romance scam:** Where a criminal poses as a potential love interest online, and the victim is persuaded to make a payment to that person after trust is established.

**Authorised push payment (APP) scam:** Where a victim is deceived into authorising a payment to an account controlled by the criminal. These would include romance scams, ‘goods not received’ scams and investment scams.

**Advance fee fraud/scam:** A subset of APP scams, specifically involving an element of emotional manipulation or social engineering to persuade victims to make financial transactions. The Crime Survey of England and Wales describes advance fee fraud as comprising “incidents where the victim is deceived or blackmailed into giving their bank card or account details to a criminal, that are then used to carry out fraud, may also be referred to as a scam.”

respondent has received a communication soliciting money for a variety of emotive reasons, for example, lottery scams, romance fraud and inheritance fraud.79

**Computer misuse:** A category of crime recorded in the Crime Survey of England and Wales and defined under the (subsequently amended) Computer Misuse Act 1990. The Crime Survey divides computer misuse into two sub-categories: computer viruses and "unauthorised access to personal information (including hacking)".

These categories are important because they are often a precursor to online fraud, with viruses and hacking used to access details that are then used to engage in fraudulent activity.

**Phishing:** Where a victim is contacted via an email that appears to be from a recognised bank or other company, attempting to trick them into entering their login details and password into a fake site with a view to using these to steal money.

**SMS phishing (SMiShing):** Where a victim is contacted via an SMS that appears to be from a recognised bank or other company, attempting to trick them into replying with their login details and password, or linking them to a fake site to enter them, with a view to using these to steal money.

**Voice phishing (vishing):** Where a victim is contacted over the telephone and persuaded to give access to personal information such as online banking login details, or to give remote access to their computer, with a view to obtaining personal information and stealing money.

**Second Payment Services Directive (PSD2):** A European Union Directive that sets requirements for banks to improve consumer protection, make payments safer and drive down the costs of payment services. As part of this, all banks will have to adopt Strong Customer Authentication, asking customers to use at least two security measures to authorise payments.

**Payment systems operators (PSOs):** Those that process payments in the banking systems. There are currently three retail PSOs – Bacs, the Cheque and Credit Clearing Company, and Faster Payments. The Payment Systems Regulator and Bank of England have established a delivery group to consolidate these systems into a single New Payment Systems Operator.

**Faster payments:** A payment system that enables mobile, internet, telephone and standing order payments to move quickly. For single payments, the money is available to the recipient within two hours, but generally takes place within minutes.

**Two-step verification:** A login process for banks and other accounts that requires both a password and a verification code that is sent to a user’s device, typically an SMS message to their mobile phone.

**Digital native:** A person who grew up in the digital age, typically of the ‘millennial’ generation.

**Cyber security:** Technologies and processes that are designed to protect devices, networks and data from cyber attacks and crimes.

**General Data Protection Regulation (GDPR):** An EU directive that sets out rules for companies that handle personal data. In May 2018, it will require all companies to report data losses within 72 hours, unless it is “unlikely to result in a risk to the rights and freedoms of data subjects”.

**Payments strategy forum:** Created by the payment systems regulator to promote collaboration within the payments industry and between stakeholders. Its members include representatives from banks, government, telecommunications companies, industry bodies and the third sector.

---
