National Audit Office

Report
by the Comptroller
and Auditor General

Home Office

Online fraud

HC 45 SESSION 2017–2019 30 JUNE 2017

Key facts

1.9m

estimated cyber-related fraud incidents in the year ending 30 September 2016 (16% of all estimated crime incidents)

623,000

actual fraud incidents recorded in the year ending 30 September 2016

£10bn

estimated loss to individuals from fraud in 2016

82%	of adults in the UK used the internet daily or almost daily in 2016
At least 6%	of adults experienced an incident of fraud in the year to 30 September 2016
In 39%	of incidents where money was taken or stolen from the victim, the loss was £250 or more in the year ending 30 September 2016
103%	increase in 'card not present' fraud, including over the internet, between 2011 and 2016, to 1.4 million cases
1 in 6	police officers' main function was neighbourhood policing in 2016
1 in 150	police officers' main function was economic crime in 2016
£130 million	of funds held in banks that cannot accurately be traced back and returned to fraud victims
27 out of 41	Police and Crime Commissioners refer to online fraud in their annual police and crime plans as at April 2017
More than 10	different education and awareness campaigns running in March 2017 to improve citizens' and businesses' cyber security

Summary

1 Growth in the use of the internet and advances in digital technologies mean that citizens and businesses can now do more online. For the UK, this means there are opportunities for greater innovation and economic growth, but also more opportunities for online crime. While traditional crimes such as vehicle offences and house burglary have declined substantially in recent years, fraud, more than half of which is committed online, is becoming more common and is a growing threat.

2 Online criminals can target thousands of victims at the same time from anywhere in the world and so are hard to trace and prosecute. Online fraud can harm citizens financially and emotionally and harm businesses' finances and reputations. The true cost of online fraud is unknown, but is likely to be billions of pounds. One estimate was that individuals lost around £10 billion and the private sector around £144 billion to fraud in 2016.

3 In the year ending 30 September 2016, the Office for National Statistics (ONS) estimated that there were 1.9 million estimated incidents of cyber-related fraud in England and Wales, or 16% of all estimated crime incidents. Online fraud includes criminals accessing citizens' and businesses' bank accounts, using their plastic card details, or tricking them into transferring money.

4 The Home Office (the Department) is responsible for preventing and reducing crime, including online fraud. Many other bodies also play a role including the police, banks, the National Fraud Intelligence Bureau (NFIB), which records fraud offences and shares information with police forces, and Action Fraud, the national reporting centre for fraud. In 2016, the Department set up the Joint Fraud Taskforce to improve collaboration between government, industry and law enforcement in tackling online fraud. In the same year, the government published its National Cyber Security Strategy to 2021, which includes the government's plans for tackling cyber crime, including cyber-enabled fraud and data theft.

Scope of this report

5 This report focuses on the Department, which is responsible for preventing and reducing online fraud. We have examined how the Department works with other bodies to tackle the crime. We have not evaluated whether the Department is achieving value for money in tackling online fraud as the true scale of online fraud and the overall cost to the government is not known. In this report we sometimes refer just to fraud as often the government and other bodies, as well as data sources, do not distinguish between online and offline fraud. We have examined:

- the nature and scale of the current threat (Part One);
- how the Department and others have responded to the threat (Part Two); and
- the challenges and opportunities the Department and others face in reducing and preventing online fraud (Part Three).

The report does not cover fiscal fraud, such as benefit fraud, committed against the government. This was covered in a National Audit Office report in 2016.[1] In addition, this report does not cover the major international cyber attack which occurred in May 2017 when we were finalising this report. The incident affected the NHS and other organisations in the UK and shows the serious risk and challenges that cyber crime presents to the UK government as well as citizens and businesses.

Key findings

Nature and scale of the threat

6 Fraud is now the most commonly experienced crime in England and Wales, and most takes place online. In the year to 30 September 2016, the ONS reported an estimated 11.8 million incidents of crime in England and Wales. For the first time, the official figures revealed an estimated 3.6 million fraud incidents, of which 1.9 million incidents (53%) were cyber-related. In the same period, there were around 623,000 fraud offences, including online fraud, recorded by the NFIB from citizens and businesses. The large difference between estimated and recorded fraud suggests that less than 20% of incidents are reported to the police. There are no official statistics on fraud losses incurred by individual banks or fraud against businesses (paragraphs 1.8, 1.9, 1.12, 1.13, 2.15 and Figure 6).

1 Comptroller and Auditor General, *Fraud landscape review*, Session 2015-16, HC 850, National Audit Office, February 2016.

7 **Online fraud is growing rapidly.** Although there are no official data to show trends in the growth of online fraud, other data indicate it is a growing crime. Criminals using stolen card details to make fraudulent transactions, including over the internet, is known as 'card not present' fraud. Known cases of this type of fraud increased by 103% between 2011 and 2016, from 709,000 to approximately 1.4 million incidents. If the current rate of growth continues, the volume of these frauds could reach 2.9 million by 2021 (paragraph 1.10 and Figure 5).

8 **Everyone is at risk of online fraud and financial losses can be serious.** In 2016, an estimated 95% of people in the UK had used the internet in the past year, as online shopping and banking grew. A survey also showed that 82% of adults in the UK used the internet "daily or almost daily" in 2016. In the same year, 60% of people banked online, compared with 35% in 2008. Emails can be used to target victims; across the world more than nine billion emails are sent every hour. In 2016, at least 6.3% of adults, or about three million people, were victims of fraud, and the crime is indiscriminate. In the year ending September 2016, in 39% of incidents where money was taken or stolen from the victim, the loss was £250 or more (paragraphs 1.4, 1.16, 1.20, 1.24 and Figure 9).

The response to the threat

9 **The face of crime is changing and needs different responses.** While traditional crimes such as burglary and vehicle offences have declined in recent years, police recorded crimes historically under-reported such as rape, the sexual exploitation of children, modern slavery, cyber crime and online fraud are now increasing. Changes in recording processes and practices by the police and an increased willingness of victims to report these crimes are thought to be driving these increases, particularly in the case of sexual offences. ONS is aiming to improve the design, coverage and presentation of crime statistics, including for fraud and cyber crime. ONS included fraud and cyber crime for the first time in annual crime figures in January 2017. There were nearly two million incidents of cyber-related fraud in 2016, 16% of all estimated crime incidents. 'Hidden' crimes require new and different responses yet, despite the level of economic crime, statistics suggest police forces remain more focused on traditional crimes. In 2016, one in six police officers' main function was neighbourhood policing, while one in 150 police officers' main function was economic crime (paragraphs 1.6 to 1.8 and 2.7).

10 **The Department has started seeing online fraud as a priority, but it is not yet a priority for all local police forces.** Since publishing its *Fraud Review* in 2006, the government has been responding to the threat of fraud in a number of ways. Online fraud now features in a number of national strategies, including the 2016 Modern Crime Prevention Strategy and the National Cyber Security Strategy. The Department also launched the Joint Fraud Taskforce in 2016, signalling its strategic commitment to fraud. Although there is an expectation for local police forces to respond to national priorities only 27 out of 41 Police and Crime Commissioners referred to online fraud in their police and crime plans as at April 2017 (paragraphs 2.2, 2.3 and 2.8).

11 The response to online fraud is uneven across the banking sector. Banks have an important role to play in protecting customers against fraud. However, the protection banks provide varies, with some investing more than others in customer education and anti-fraud technology. In 2016, the Payment Systems Regulator found that banks needed to improve the way they work together in responding to scams, that some banks needed to do more to combat scams, and that data available on the scale of scams were poor. Some fraud relating to scams is included within overall fraud loss figures, but it is not reported separately. Other data available suggest that somewhere between 40% and 70% of people who are victims of scams do not get any money back. Banks are reported to be holding at least £130 million of funds that cannot accurately be traced back and returned to fraud victims (paragraphs 2.9 and 2.10).

12 Setting up the Joint Fraud Taskforce, led by ministers, was a positive step, but its success relies on voluntary participation from industry and law enforcement. The Department has shown good leadership by bringing together key stakeholders across a complex landscape. However, in leading the response to online fraud, it has to influence Taskforce partners to take responsibility in the absence of more formal legal or contractual levers. Beyond the oversight provided by the Taskforce's Management Board and Oversight Board, chaired by the Home Secretary, there is a lack of proper governance, such as through a senior responsible owner or equivalent role. Despite setting up the Taskforce in February 2016, the Department has not yet reported on the Taskforce's progress or established measures for its performance (paragraphs 2.12 and 2.14 to 2.16).

13 The Joint Fraud Taskforce has too narrow a focus on banking. At present, only banks represent industry on the Taskforce. However, many other organisations, including those in the retail, telecommunications and digital sectors, have responsibilities for preventing and reducing online fraud (paragraph 2.13 and Figure 12).

Challenges and opportunities to tackle online fraud more effectively

Prevention

14 There is a lack of co-ordination and consistency in education campaigns to improve citizens' and businesses' cyber security. The growing scale of online fraud suggests that many people are still not aware of how to keep safe online and that there is more to do to change citizens' and businesses' behaviour. As at 31 March 2017, the government and other bodies were running more than 10 different education and awareness campaigns to improve citizens' and businesses' cyber security. Different organisations running campaigns, with slightly different messages not tailored for specific groups, can confuse the public and reduce the impact of the campaigns. The Department is evaluating one fraud awareness campaign, but the evaluation will not be completed until March 2018 (paragraphs 3.3 to 3.7 and Figure 13).

15 Although educating people to stay safe online is sensible, the Department considers that government and industry have responsibility to protect citizens and businesses. The Department considers that education is one element of preventing online fraud, but that government also needs to make the internet and email more secure, while banks and other organisations have responsibility to protect customers' data. To this end, as part of its wider responsibilities for national cyber security, the National Cyber Security Centre is seeking to stop spoof emails and take down spoof websites that can lead to online fraud. The banks, meanwhile, are improving their IT systems to protect their customers and money from online fraudsters, (paragraphs 2.2, 2.9 and 3.8).

16 There is no clear mechanism for identifying, developing and sharing good practice to prevent people becoming victims. There are examples of good practice in protecting people against online fraud. These include Sussex Police's initiative to help bodies such as banks and charities identify potential victims, and Canada's peer-to-peer support network for vulnerable old people. However, it is not clear where the police and other stakeholders can easily find and share good practice (paragraph 3.9).

Reporting

17 Without accurate data, the Department does not know whether its response is sufficient or adequate. Not only is online fraud under-reported, but where data are available, there is a lack of sharing of information between government, industry and law enforcement agencies. For example, there is no formal requirement for banks to report fraud or share reports with government. Action Fraud and the NFIB plan to introduce an enhanced system for collecting and analysing data later in 2017 to help the government and others understand the threat. However, the success of the new database will depend on whether the data reported to Action Fraud are comprehensive, accurate and timely. The National Cyber Security Centre also aims to generate useful data to share with others through its work on internet defence (paragraphs 3.10 to 3.14 and Figure 14).

Disruption

18 People spend money in increasingly diverse and complex ways, and criminals continually innovate, meaning there is no single solution to designing out fraud. The Department and banks recognise there is no single solution, like Chip and PIN 10 years ago, to reduce online card fraud. As more people use cards to make payments online rather than in person, criminals have used this vulnerability by stealing people's card details and using them many times. One plan to address this type of fraud is to introduce cards that change their security code (the number on the back of the card) every hour to prevent the use of stolen card data. This is a positive step, as the re-design may help to stop an increase in online card fraud. However, such a plan requires all card providers to participate. In addition, the Department will need to continue to work with industry to innovate as criminals find other ways to attack vulnerabilities (paragraphs 3.17 and 3.18).

19 The Department, through the Taskforce, is seeking to deny criminals access to their proceeds from fraud. Advances in payment systems, such as faster payments, make it easier for criminals to receive and distribute the proceeds of fraud through multiple accounts at speed, knowing that it is difficult for banks to identify and stop funds, and return them to victims. The Department, with other partners on the Taskforce, is examining how these flows of money can be identified and stopped more easily, but this initiative will rely on all banks participating (paragraphs 3.18 and 3.19).

Prosecution

20 The nature of online fraud makes it difficult to pursue and prosecute criminals. Although the government wants the police and judiciary to make greater use of existing laws, and stakeholders agreed it was possible to use existing laws to prosecute online fraud cases, the government needs to ensure that current legislation remains applicable in the face of continual technological change and rapidly evolving threats. The international and 'hidden' nature of online fraud makes it difficult to pursue and prosecute criminals because of the need for international cooperation and an ability to take action across borders. The City of London Police oversees Action Fraud and the National Fraud Intelligence Bureau (NFIB) and leads on reporting and intelligence functions for all frauds and cyber crimes. As the national lead force for fraud, it is also responsible for improvement in capability at the local level, and investigating or offering assistance in cases of complex frauds. The National Crime Agency is responsible for leading, supporting and coordinating the response to serious and organised economic crime, including cyber-enabled fraud. The Agency, for example, targets enablers of fraud, such as network intrusions, which can yield large amounts of personal information (paragraphs 2.5, 3.20, 3.21 and 3.24).

21 There is a lack of data on how many fraudsters are prosecuted; there are also concerns about the sentences fraudsters receive. The prosecution rate for online fraud is low due to the hidden nature of the crime. However, there is also a lack of information on judicial outcomes for fraud offences, as data cannot easily be matched across the Department and the Ministry of Justice. According to some stakeholders, criminals do not always receive sentences proportionate to the crime, particularly in relation to the non-financial harm victims suffer (paragraphs 3.22 and 3.23).

Conclusion

22 For too long, as a low-value but high-volume crime, online fraud has been overlooked by government, law enforcement and industry. It is a crime that can affect everyone. Fraud is now the most commonly experienced crime in England and Wales, is growing rapidly and demands an urgent response. Yet fraud is not a strategic priority for local police forces, and the response from industry is uneven.

23 The Department is not solely responsible for reducing and preventing online fraud but is the only body that can oversee the system and lead change. Getting the right balance of resources to respond to the threat of online fraud remains a challenge. The national picture of crime continues to change and responsibilities for tackling online fraud are often unclear. The Department's launch of the Joint Fraud Taskforce in February 2016 was a positive step, but there is still much work to be done. At this stage it is hard to judge that the response to online fraud is proportionate, efficient or effective.

Recommendations

a To promote transparency and accountability, the Department should:

- with other Taskforce partners, including banks and law enforcement agencies, publish information on the Joint Fraud Taskforce's performance and future plans;
- identify and implement suitable accountability arrangements, including within the Joint Fraud Taskforce, so that the responsibilities of all partners for preventing and reducing online fraud are clear; and
- expand the membership of the Joint Fraud Taskforce to include other stakeholders, such as the retail and digital sectors.

b The Department, with Joint Fraud Taskforce partners, should establish arrangements for identifying, measuring and tracking the benefits of its initiatives to reduce fraud, including setting baselines.

c To address intelligence gaps, the Department, working with the City of London Police and banks, should improve the collection and reporting of data on fraud.

d The Department should work with Police and Crime Commissioners and chief constables to identify and share good-practice models of policing for tackling online fraud, and support forces in making fraud a strategic priority. To support this activity, the Department should commission HM Inspectorate of Constabulary to undertake a national thematic inspection of police forces' performance in tackling fraud.

e The Department should work with the Ministry of Justice to:

- improve data on fraud prosecutions to help inform future investigations and prosecutions; and
- examine sentencing guidelines on fraud, and whether the impact on vulnerable victims is taken into account sufficiently in sentencing.