National Audit Office

Report
by the Comptroller
and Auditor General

Home Office

Online fraud

HC 45 SESSION 2017–2019 30 JUNE 2017

Our vision is to help the nation spend wisely.

Our public audit perspective helps Parliament hold government to account and improve public services.

The National Audit Office scrutinises public spending for Parliament and is independent of government. The Comptroller and Auditor General (C&AG), Sir Amyas Morse KCB, is an Officer of the House of Commons and leads the NAO. The C&AG certifies the accounts of all government departments and many other public sector bodies. He has statutory authority to examine and report to Parliament on whether departments and the bodies they fund have used their resources efficiently, effectively, and with economy. Our studies evaluate the value for money of public spending, nationally and locally. Our recommendations and reports on good practice help government improve public services, and our work led to audited savings of £734 million in 2016.

National Audit Office

Home Office

Online fraud

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 28 June 2017

This report has been prepared under Section 6 of the National Audit Act 1983 for presentation to the House of Commons in accordance with Section 9 of the Act

Sir Amyas Morse KCB
Comptroller and Auditor General
National Audit Office

22 June 2017

HC 45 | £10.00

This report examines the nature and scale of online fraud, how the Home Office (the Department) and others have responded to the threat, and opportunities for the Department and others to tackle online fraud more effectively.

11473 06/17 NAO

Contents

The National Audit Office study team consisted of:
Benjamin Bernard, Harry Hagger Johnson, Helen Hodgson, Linda Mills, Sonia Coates, Hugh Turner, Charmaine Lartey and Tom Diamond, under the direction of Louise Bladen.

This report can be found on the National Audit Office website at www.nao.org.uk

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157–197 Buckingham Palace Road
Victoria
London
SW1W 9SP

Tel: 020 7798 7400

Enquiries: www.nao.org.uk/contact-us

Website: www.nao.org.uk

Twitter: @NAOorguk

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.

Part One

Nature and scale of the threat

1.1 This part examines the nature and scale of the threat of online fraud. It describes:

- the nature of online fraud;
- the scale of online fraud; and
- why citizens and businesses are at risk.

The nature of online fraud

1.2 Online crime differs from traditional crimes, such as vehicle offences or house burglary, as shown in **Figure 1**. It presents a greater challenge to government, law enforcement and industry. Fraud can be committed "by false representation", "by failing to disclose information" or "by abuse of position for gain or to cause a loss".[2] Our report focuses on online fraud, where fraud is committed in whole or partly online.

1.3 Online criminals can target victims remotely from anywhere in the world. They can target thousands of people at the same time, quickly and anonymously. Criminals constantly innovate to take advantage of people and exploit weaknesses in emerging technologies. Criminals are unlikely to be traced and prosecuted. **Figure 2** on page 14 sets out an example of how criminals can commit online fraud.

1.4 Criminals can commit online fraud in a number of ways. They can initiate the crime offline by stealing a credit card, or by contacting someone by post or by phone. They can also initiate the crime through the internet, via social media or emails, or by accessing data held by banks or other organisations. Criminals do this by:

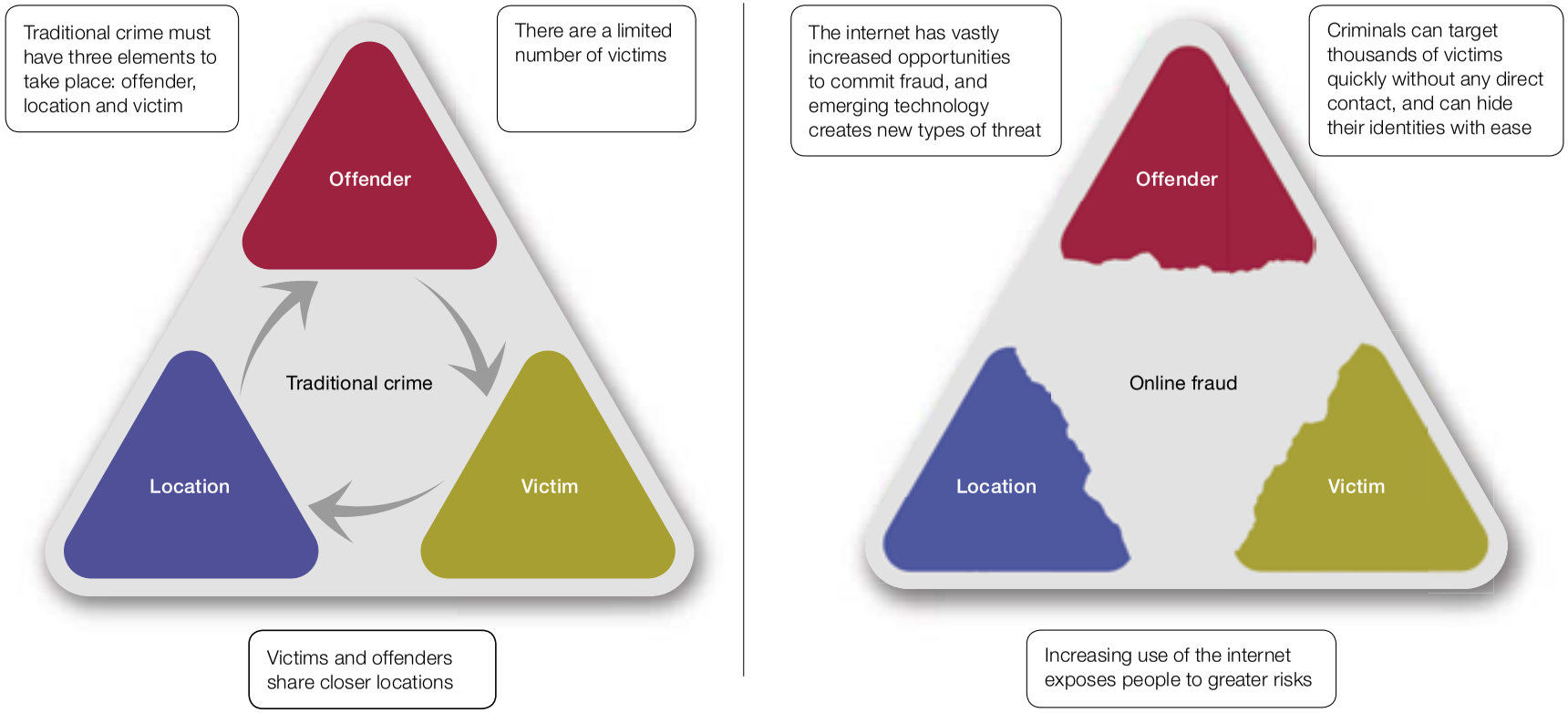
- phishing (sending spoof emails to encourage victims to enter sensitive information on a fake website);
- social engineering (deceiving individuals into sharing sensitive personal information);
- malware (malicious software designed to gain access to sensitive information); or
- illegally purchasing personal data.

2 Fraud Act 2006.

Figure 1

Why online crime is a greater challenge than traditional crime

New technologies and increasing use of the internet mean online crime can happen on a greater scale, at a faster speed and reach more victims than traditional crime

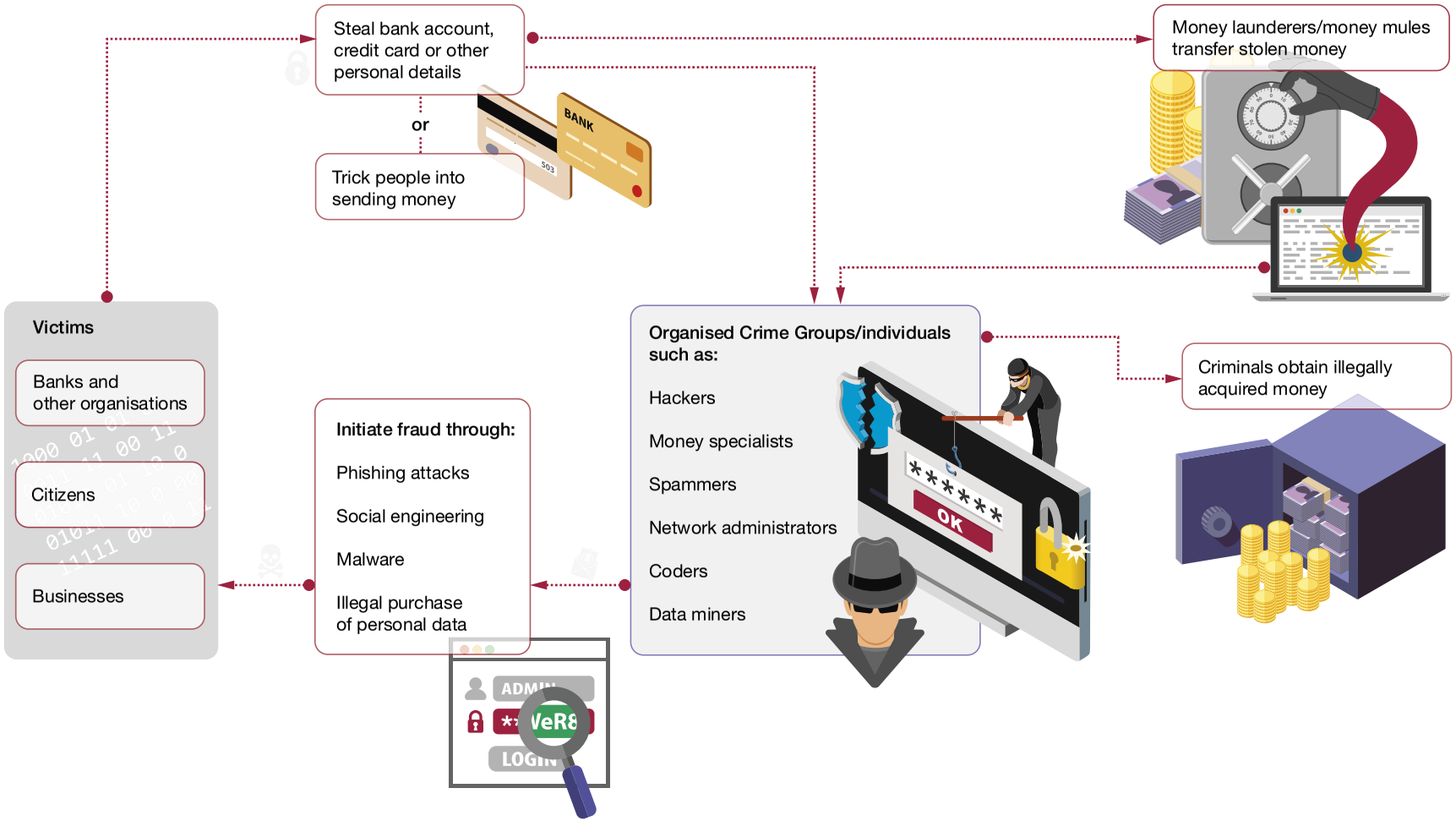


Source: National Audit Office analysis and Home Office, *Modern Crime Prevention Strategy*, March 2016

Figure 2

An example of how criminals commit online fraud

Criminals often have sophisticated business operations to commit online fraud



Source: National Audit Office

1.5 A criminal may start by contacting their victim online, but then the fraud may continue online or move offline, as can be the case with romance fraud. **Figure 3** sets out some examples of online fraud – from criminals stealing and using credit card details online to criminals tricking people into sending them money.

The scale of online fraud

1.6 In the past, burglary and vehicle offences were the main high-volume crimes, according to crime statistics. However, as incidences of traditional crimes have fallen, some police recorded crimes, under-reported in the past, such as rape, the sexual exploitation of children, modern slavery, cyber crime and online fraud, are now increasing. According to the Office for National Statistics (ONS) 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 for England and Wales, including for fraud and cyber crime. ONS included fraud and cyber crime for the first time in annual crime figures in January 2017. Continuing improvement in the statistics on fraud and cyber crime highlighting the extent of the problem should help the Home Office to be better placed to take action where needed. These 'hidden' crimes can require new and different police responses.

Figure 3
Examples of online fraud

Criminals can commit many different types of fraud online

Fraud type	Definition
Plastic card fraud	A stolen card, or personal information stolen from a card, is used to commit fraud online. Fraudsters use the cards or details to purchase goods, or obtain unauthorised funds from accounts.
Mandate fraud	Fraudsters obtain details of direct debits, standing orders or account transfer details and amend them to transfer monies to other accounts.
'419' advance fee fraud	A communication soliciting money from the victim for a variety of emotive reasons to assist the fraudster.
Romance fraud	The victim is befriended on the internet and eventually convinced to assist their new love financially, by sending them money.
CEO fraud	A fraudster sends an email to a staff member in a company's finance department. The fraudster, purporting to be a company director or chief executive officer, tells the staff member to quickly transfer money to a bank account for a specific reason.
Lottery scam	The victim is informed that they have won a lottery, which is non-existent, and are required to send an advance fee to release their winnings.
Ransomware	A type of malicious software that carries out an extortion attack that blocks access to data until a ransom is paid. Payment may unblock data or access to data may continue to be withheld.
Investment fraud	Used to describe a variety of scams offering income, interest or profit in return for financial investment. Fraudsters target potential investors with share sales, wine investments, rare goods and other products. Such investments are often, in fact, unregulated, overpriced, high risk and difficult to sell on.

Source: *Home Office counting rules for recorded crime*, April 2016; Action Fraud, *A-Z of Fraud; Action Fraud news*, February 2016

The decline in traditional crime

1.7 **Figure 4** shows that, from 2002-03 to 2015-16, burglary and vehicle offences were on a general downward trend. In 2002-03, there were more than one million recorded vehicle offences, but such offences fell by 66% to 366,288 offences in 2015-16.

The rise in online fraud

1.8 Although there are no robust national statistics on how the level of online fraud has changed over time, data published in January 2017 showed that fraud, including online fraud, is now the most commonly experienced crime in England and Wales. In the year ending 30 September 2016, there were an estimated 11.8 million incidents of crime in England and Wales, of which:

- 6.2 million (52%) related to crimes against the person (for example, violence or theft from the person) and against households (for example, domestic burglary or criminal damage). This figure was unchanged from the previous year;
- 3.6 million (31%) related to fraud, including bank and credit account fraud, non-investment fraud, advance fee fraud and other fraud. Of this 3.6 million, 1.9 million incidents (53%) were cyber-related, meaning the internet or any type of online activity was related to any aspect of the incident; and
- 2.0 million (17%) related to computer misuse, including unauthorised access to personal information and hacking.[3]

1.9 There is no comparable estimate of fraud against businesses in England and Wales because the Crime Survey for England and Wales is a household survey.

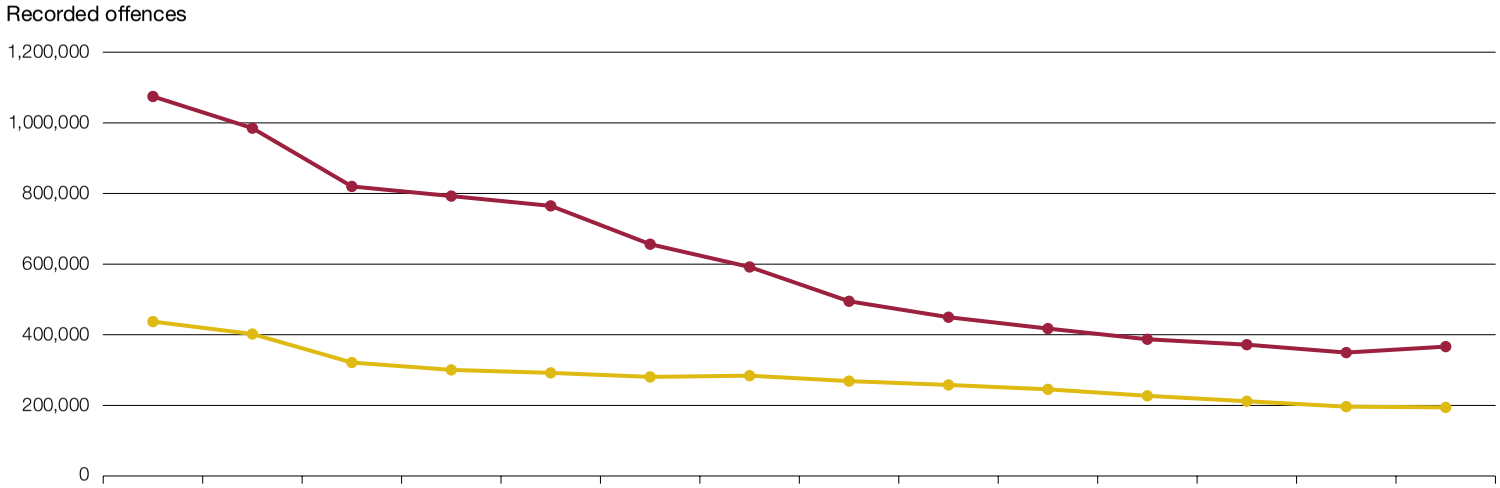
1.10 Although there are no official data on growth trends in online fraud, other industry data on financial fraud show an upward trend. In 2016, there were 176 million credit and debit cards in the UK.[4] There were also approximately 1.4 million cases of 'card not present' fraud, compared with 709,000 in 2011, an increase of 103% (**Figure 5** on page 18).[5] This type of fraud involves criminals using card details obtained fraudulently to make purchases, including over the internet. If the current rate of growth continues, the volume of these frauds could reach 2.9 million by 2021.

3 Office for National Statistics, *Crime in England and Wales: year ending Sept 2016*, January 2017.
4 The UK Cards Association, *UK card payments 2016*, 2016.
5 Financial Fraud Action UK, *Fraud the Facts 2016: The definitive overview of payment industry fraud*, 2016.

Figure 4

Recorded offences in England and Wales for domestic burglary and vehicle offences, 2002-03 to 2015-16

Domestic burglary and vehicle offences have been on a downward trend since 2002-03



	2002-03	2003-04	2004-05	2005-06	2006-07	2007-08	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16
Vehicle offences	1,074,659	985,006	820,096	792,821	765,015	656,453	591,853	494,873	449,616	417,442	387,359	372,041	349,555	366,288
Domestic burglary	437,583	402,345	321,507	300,517	292,260	280,696	284,431	268,606	258,165	245,312	227,276	211,988	196,557	194,412

Notes

1 Domestic burglary includes actual and attempted residential burglaries, including distraction burglaries, in England and Wales. Prior to 2009-10, there was a single burglary definition known as 'burglary in a dwelling'.

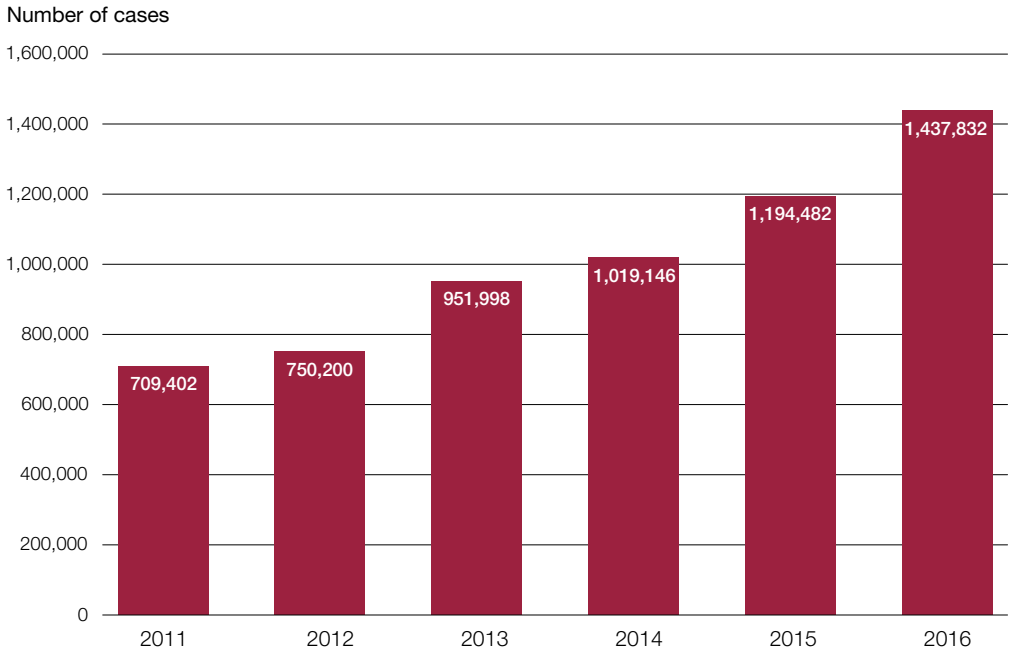
2 Vehicle offences include 'aggravated vehicle taking', 'theft from a vehicle', 'theft of or unauthorised taking of a motor vehicle' and 'vehicle interference'.

Source: National Audit Office analysis of Police Recorded Crime data

Figure 5

Annual volume of 'card not present' fraud on UK issued cards, 2011 to 2016

The volume of 'card not present' fraud increased by 103% between 2011 and 2016



Note

1 The number of frauds relates to the number of cards that have been defrauded, rather than the number of victims.

Source: National Audit Office analysis of Financial Fraud Action UK data, *Fraud the Facts 2016: The definitive overview of payment industry fraud*, 2016 and *Year-end 2016 Fraud update: Payment cards, remote banking and cheques*

1.11 Losses associated with 'card not present' fraud through the internet were £308.8 million in 2016.[6] This is a 134% increase since 2011 (£139.6 million). If the current rate of growth continues, 'card not present' fraud losses could exceed £680 million by 2021. Although this growth in fraud mirrors growing card ownership, at the same time criminals are making more money from fraud.

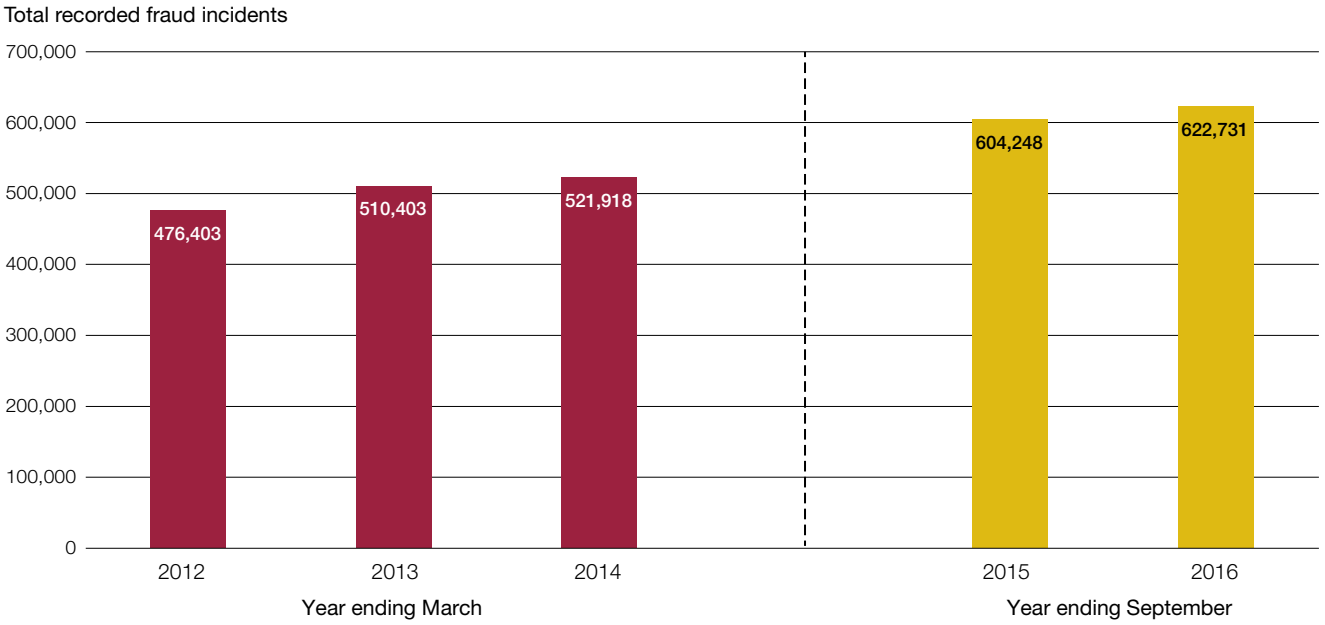
1.12 In the year ending 30 September 2016, around 623,000 fraud offences were reported, 3% more than in the previous year.[7] The number of incidents reported to the police has increased year-on-year since April 2011, although this could indicate increased reporting, as well as increasing crime levels (**Figure 6**).

6 See footnote 5.
7 Office for National Statistics, *Fraud offences recorded by the National Fraud Intelligence Bureau*, January 2017.

Figure 6

Recorded fraud from April 2011 to September 2016

The number of fraud incidents recorded by the police is rising



Notes

1 Action Fraud and the National Fraud Intelligence Bureau, which are part of the City of London Police, collect and record reported fraud.

2 Regarding 2012 to 2014 data, from 2011, Action Fraud started recording fraud offences on behalf of individual police forces and took over full responsibility from April 2013. These figures include offences recorded by either police forces or Action Fraud separately, or both, depending on the time period specified.

3 Data for 2015 and 2016 are based on figures recorded by the National Fraud Intelligence Bureau, and analysed by the Office for National Statistics.

4 Data from each period include reports made by Cifas and Financial Fraud Action UK, although these organisations only record cases from their members.

Source: National Audit Office analysis of Office for National Statistics data, *Crime in England and Wales: Bulletin Tables*

1.13 Most frauds are not reported to the police. The number of reports is much lower than the estimate of 3.6 million fraud incidents over the same period (paragraph 1.8). This suggests that only around 20% of victims of fraud report incidents. Fraud is not reported for a number of reasons. Citizens and businesses may:

- not be aware that they have been targeted;
- not regard themselves as victims, or consider their losses too small to report;
- be too embarrassed to come forward;
- not be aware of how to report fraud; or
- find the reporting process not relevant or too complicated and drop out.

1.14 In 2016, the Payment Systems Regulator reported that the data available on the scale and types of scams where people are tricked, often online, into making payments to fraudsters are of poor quality. The Payment Systems Regulator's view was that the initial evidence available suggested the scale of the crime may be significant, and the general view was that the prevalence of such scams was likely to increase.[8]

1.15 Although banks are not required to publish or report fraud losses in their annual reports, they do submit their fraud loss figures to Financial Fraud Action UK, whose members includes the major retail banks and card issuers. Financial Fraud Action UK produces aggregate industry fraud figures covering payment card, remote banking and cheque fraud, which it publishes twice a year. The aggregate figures are also submitted to the Office for National Statistics (ONS) and included in quarterly crime figures.

Why citizens and businesses are at risk

1.16 In 2016, 95% of people in the UK were estimated to have used the internet in the past 12 months, and across the world, more than nine billion emails are sent every hour.[9] In addition, data from the ONS show that:

- 82% of people used the internet "daily or almost daily" in 2016, compared with 49% in 2008;
- 77% of people had shopped online within the past 12 months in 2016, compared with 53% in 2008; and
- 60% of people had carried out banking online within the past three months in 2016, compared with 35% in 2008 (**Figure 7**).[10]

1.17 In recent years, people have moved away from using computers to access the internet, and a growing number now own smartphones and tablets. This means that people can carry out more transactions in public and over less secure internet connections, where data breaches can occur. **Figure 8** on page 22 shows that, of adults in the UK, in 2016:

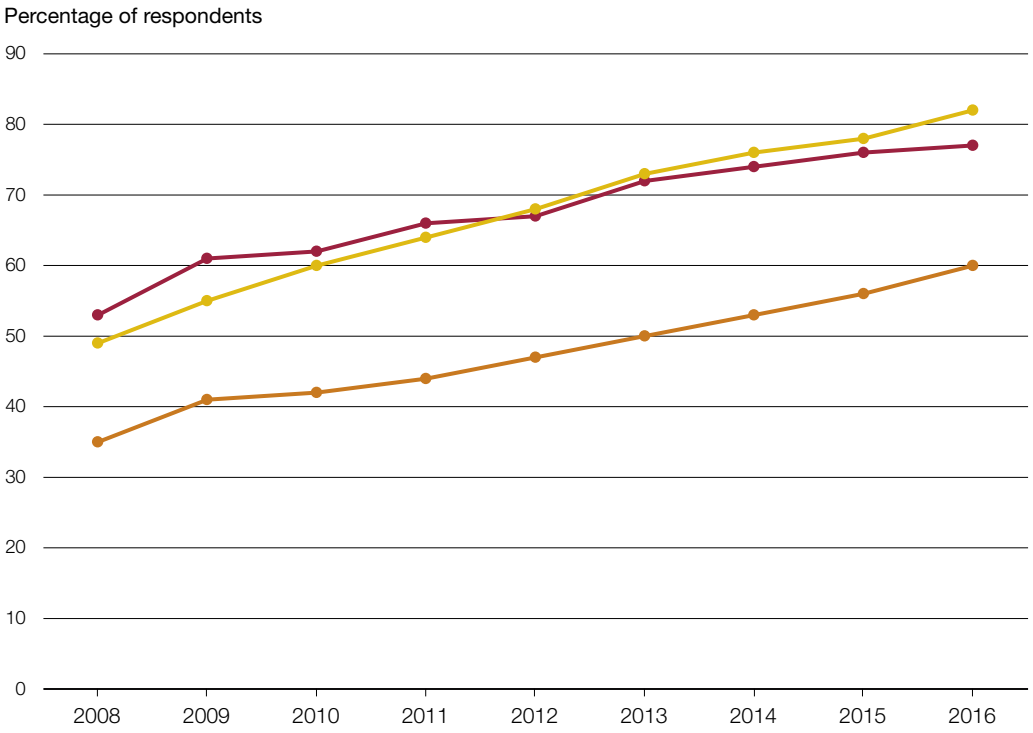
- 71% had a smartphone, compared with 27% in 2011; and
- 59% had a tablet, compared with 2% in 2011.[11]

8 Payment Systems Regulator, *Which? authorised push payments super-complaint: Payment Systems Regulator's response*, December 2016.
9 National Audit Office analysis of Eurostat data, ICT usage in household and by individuals. Based on internet use by individuals aged 16 to 74.
10 National Audit Office analysis of Office for National Statistics data, *Opinions and Lifestyle Survey, Internet access – households and individuals 2016*.
11 Ofcom, *Communications Market Report 2016*, August 2016.

Figure 7

Trends in consumer activities online from 2008 to 2016

An increasing percentage of people are shopping and banking online



	2008	2009	2010	2011	2012	2013	2014	2015	2016
Shopping online within past 12 months	53	61	62	66	67	72	74	76	77
Internet use "daily or almost daily"	49	55	60	64	68	73	76	78	82
Internet banking within past three months	35	41	42	44	47	50	53	56	60

Note

1 These data are from the Opinions and Lifestyle Survey, a household survey conducted in Great Britain.

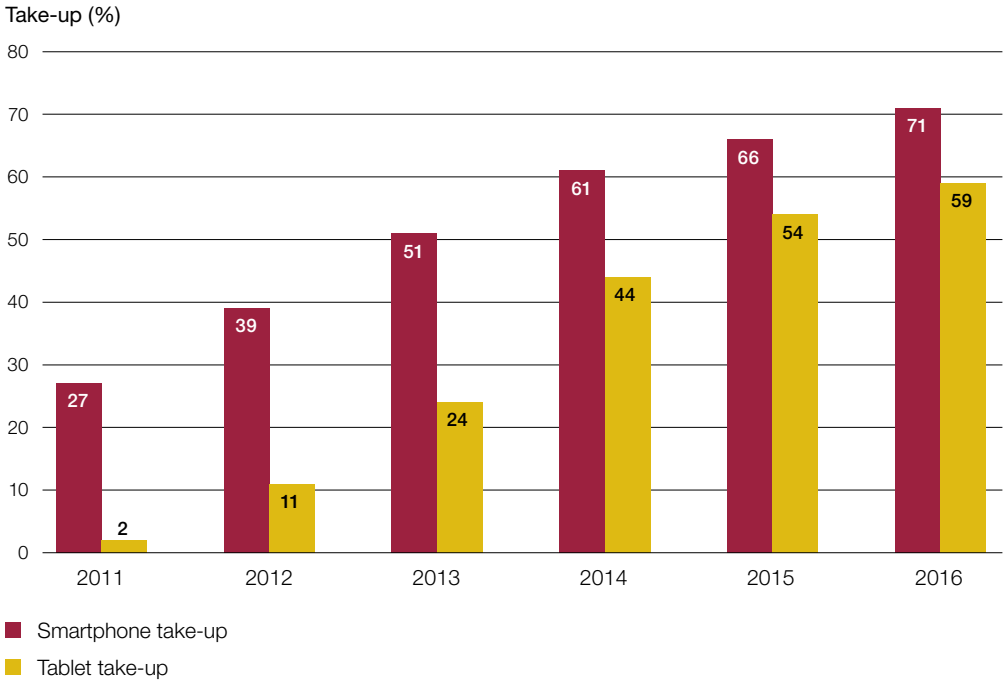
Source: National Audit Office analysis of Office for National Statistics data, *Opinions and Lifestyle Survey, Internet access – households and individuals 2016*

1.18 The rapid growth in the use of the internet described above creates increasing opportunities for criminals to commit fraud against citizens and businesses. People:

- are at increasing risk of being defrauded in many different ways;
- can access their money in many different ways; and
- can transfer money quickly, often immediately.

Figure 8
Smartphone and tablet take-up, 2011 to 2016

Take-up of internet-enabled smartphones and tablets is increasing



Note

1 The Ofcom survey's effective weighted sample size for smartphones was 2,318; for tablets the effective weighted sample size was 2,504.

Source: National Audit Office analysis of Ofcom data, *Communications Market Report 2016*, August 2016

1.19 To protect themselves against online fraud, citizens and businesses need to take precautions, such as keeping their software up to date and being wary of scams. A current campaign called Take Five advises people not to disclose security details and not to assume emails are authentic.

How fraud affects citizens and businesses

1.20 Fraud is the most prevalent crime, and people are about nine times more likely to be a victim of fraud than of theft from the person, and about four times more likely to experience fraud than violent crime.[12] Anyone in society can be a victim of fraud, and there is less difference between victims' personal characteristics than for other crimes. In the year to 30 September 2016, 6.3% of adults, or about three million people, were victims of fraud. This included:

- 6.5% of men, compared with 6.2% of women;
- 8% of adults in managerial and professional occupations, compared with 5% in routine or manual occupations;
- 7.6% of adults with degrees or diplomas, compared with 3.4% with no qualification; and
- 7.9% of adults aged 25 to 34 years, compared with 3.3% aged over 75 years.[13]

1.21 The large majority of victims of fraud had been a victim only once (85%), but hundreds of thousands of cases involve repeat victimisation. For example, of victims of bank and credit account fraud, 14% experienced repeat incidents during the year.[14] Stakeholders also told us that some citizens are more vulnerable to some frauds, such as romance fraud, at certain points in their lives, for example following bereavement, separation or job loss. Online fraud can harm citizens emotionally as well as financially.

1.22 Online fraud harms businesses' finances and reputations. Large businesses are more likely to have the skills, experience and resources to protect themselves against online fraud because the risk of becoming a victim depends on how sophisticated a business's internal process and financial control environments are. In contrast, small and medium-sized enterprises (SMEs) often have less capacity and capability to defend themselves against online fraud. In 2016, there were 5.5 million businesses in the UK, of which 99.3% were small businesses.[15]

12 Office for National Statistics, *Crime statistics for England and Wales, year ending September 2016*, January 2017. Bulletin tables.
13 Office for National Statistics, *Crime statistics for England and Wales, year ending September 2016*, January 2017. Additional experimental tables on fraud.
14 Office for National Statistics, *Statistical bulletin: Crime in England and Wales, year ending September 2016*, January 2017.
15 Department for Business, Energy & Industrial Strategy, *Business population estimates for the UK and regions 2016 – statistical release*, October 2016.

1.23 In terms of the financial impact of fraud, of the estimated 3.6 million incidents of fraud committed against individuals in the year to 30 September 2016, 2.4 million incidents (66%) involved an initial loss of money or goods, independent of any reimbursement received.[16] Of these 2.4 million incidents:

- 1.7 million (71%) were incidents where victims received a full reimbursement, typically from their financial provider. In 703,000 cases, the victim received no or partial reimbursement; and
- incidents of bank and credit account fraud were more likely to result in initial loss to the victim (73%, equivalent to 1.8 million incidents) than were other types of fraud. In the majority of these incidents, the victim received a full reimbursement (83%). In 43% of non-investment frauds (such as fraud related to online shopping scams), there was no loss to the victim. This compares with 27% of incidents of bank and credit account fraud where no loss was suffered.[17]

1.24 The value of individual fraud cases varies, although 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 (**Figure 9**).

1.25 The true overall cost of online fraud is unknown. In 2016, the Annual Fraud Indicator estimated that individuals lost around £10 billion and the private sector around £144 billion to fraud.[18] There are other estimates of the cost of fraud to the UK economy and to victims in total:

- In 2016, the British Retail Consortium crime survey estimated that 53% of reported fraud in the retail industry was 'cyber-enabled', equivalent to losses of £100 million.[19]
- In 2015, Financial Fraud Action UK reported that fraud relating to online and phone banking, debit and credit cards, and cheques was £755 million, a 26% increase on 2014.[20]

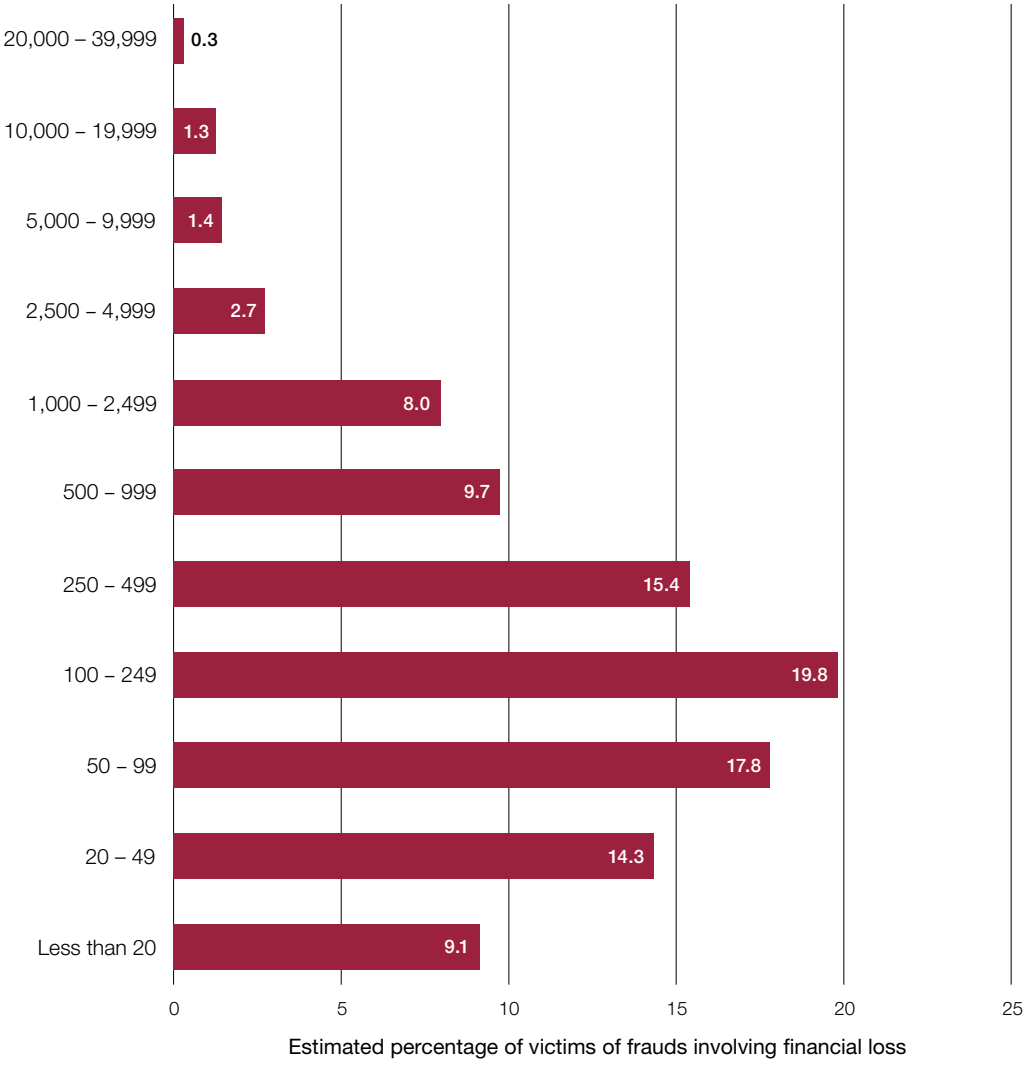
1.26 Serious organised crime groups are actively engaged in fraud and may use the proceeds from fraud to fund other criminal activities. There have been a number of links between fraud and the funding of terrorist activities. A recent case showed how a number of smaller frauds totalling £1 million was used to fund travel to the conflict in Syria.

16 This refers to both money taken or stolen by the fraudster as well as any additional costs or charges as a consequence of the fraud, such as bank charges, repair costs and replacement costs.
17 See footnote 13.
18 University of Portsmouth, PKF Accountants & business advisers and Experian, *Annual Fraud Indicator 2016*, May 2016.
19 British Retail Consortium, *2016 Retail Crime Survey*, February 2017.
20 Financial Fraud Action UK, *Fraud the Facts 2016: The definitive overview of payment industry fraud*, 2016.

Figure 9

Estimated loss per fraud against citizens in year to September 2016

Of fraud victims, 39% suffered a financial loss of £250 or more



Notes

1 Figures exclude frauds with no monetary loss and frauds against businesses.

2 Figures are for all frauds, not just online fraud.

Source: Office for National Statistics, *Crime statistics for England and Wales, year ending September 2016*. Additional experimental tables on fraud

Part Two

The government's response to the threat

2.1 This part examines government's approach, led by the Home Office (the Department), to tackle online fraud. It sets out:

- the government's response to the threat of online fraud;
- the Department's roles and responsibilities; and
- how the Department works with others to prevent, record, disrupt and prosecute online fraud.

The government's response to fraud over time

2.2 In 2006, the government published the *Fraud Review*, which examined ways of reducing fraud. Among other things, the review recommended that the government should:

- establish the National Fraud Strategic Authority;
- establish a national fraud reporting centre for businesses and individuals;
- work with others to run public awareness and education campaigns; and
- take steps to improve the police response to investigating fraud.

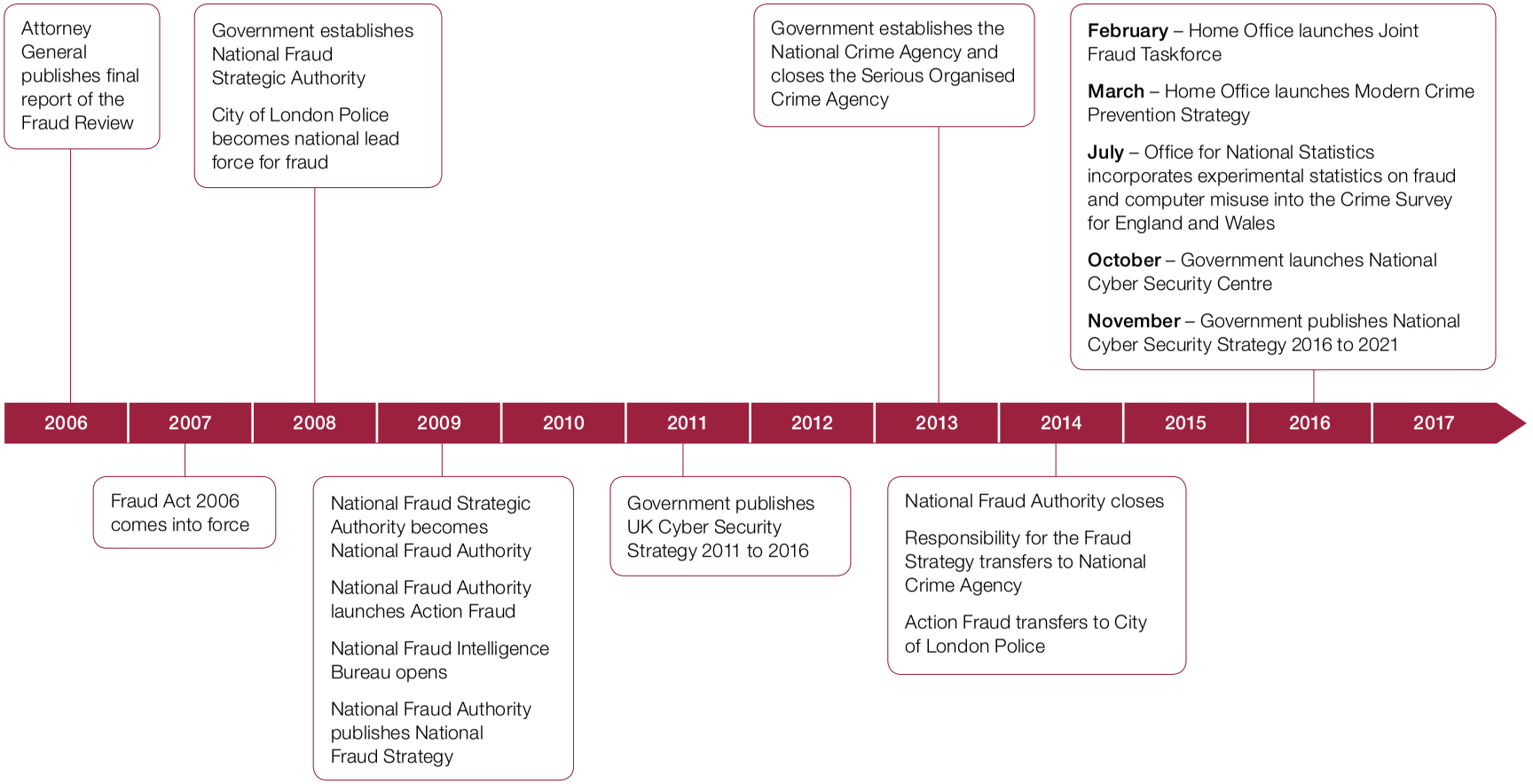
2.3 **Figure 10** sets out how the government has responded to the threat of online fraud since 2006, when the Fraud Act came into force. This act introduced the offence of fraud for the first time.

- In 2008, the Department set up the National Fraud Strategic Authority (later the National Fraud Authority) to lead and coordinate efforts to reduce fraud. The Authority set up Action Fraud as the UK's national reporting centre for fraud.
- In 2011 and 2016, the government published the first and second National Cyber Security Strategies.
- In 2014, the Department closed the Authority because it wanted to strengthen the government's work to tackle economic crime by concentrating effort into law enforcement bodies. The City of London Police, the national policing lead for fraud, took over responsibility for Action Fraud.
- In February 2016, the Department set up the Joint Fraud Taskforce.

Figure 10

Timeline of government's response to the threat of online fraud

Over the past 10 years the government has introduced various reforms to tackle online fraud



Source: National Audit Office analysis

Roles and responsibilities of the Department and others

2.4 The Department is responsible for reducing and preventing crime, including online fraud. Growth in online fraud, however, presents new and significant challenges for the Department, as many other government bodies, law enforcement agencies and industry play a role. These roles are set out in **Figure 11**.

2.5 The bodies involved, include:

- City of London Police which oversees Action Fraud (the UK's national reporting centre for fraud and cyber crime) and the National Fraud Intelligence Bureau (NFIB) leading on reporting and intelligence functions for all frauds and cyber crimes. City of London Police as the national lead force for fraud is responsible for driving improvements in capability at the local level, and investigating or offering assistance in cases of complex frauds.
- police forces, which are responsible for reporting fraud cases to Action Fraud and investigating cases referred to them by the NFIB;
- Police and Crime Commissioners, who set their local force's policing priorities and work with local partners to prevent crime;
- the National Crime Agency, which leads, supports and coordinates the response to serious and organised economic crime, including cyber-enabled fraud. For example, the Agency targets enablers of fraud, such as network intrusions, which can yield huge amounts of personal information. The Agency includes the National Cyber Crime Unit;
- National Trading Standards, which enforces laws to protect consumers from online frauds involving the sale of counterfeit or non-existent goods;
- industry, including banks and the retail sector, which has a role in preventing, reporting and disrupting fraud; and
- other government departments and agencies, including the Cabinet Office, responsible for UK cyber security, and the National Cyber Security Centre.

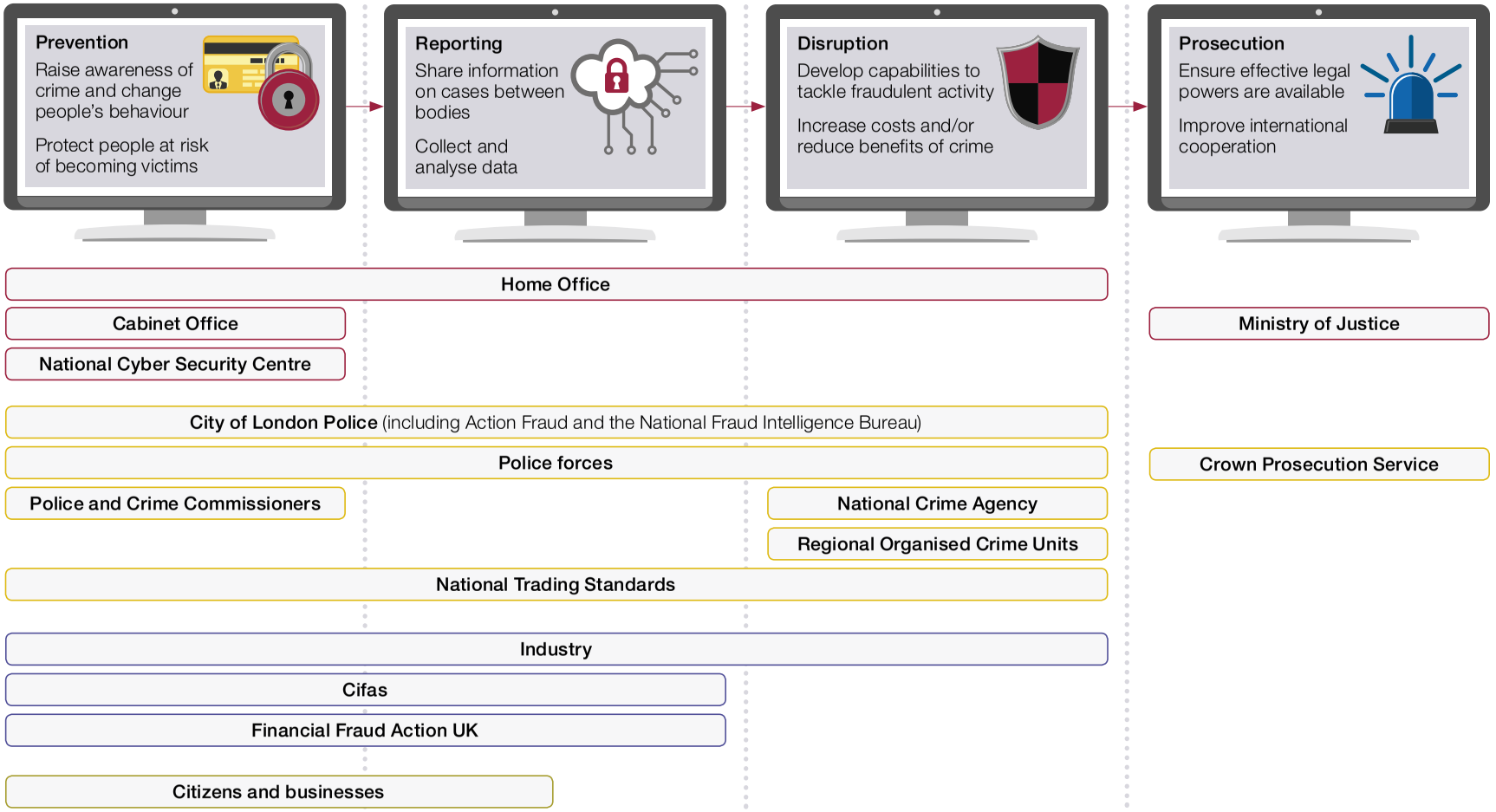
The Department's work to reduce the impact of online fraud is part of the government's wider National Cyber Security Strategy to reduce the impact of cyber crime on the UK. In particular, the Department's work supports the Strategy's objectives of:

- changing public and business behaviours; and
- reducing cyber crime.

Figure 11

Roles and responsibilities for online fraud

The Department works with others from government, law enforcement and industry to tackle online fraud



Note

1 The Department is included under 'Recording' and 'Disruption' to indicate areas of oversight.

Source: National Audit Office analysis

The police response

2.6 The City of London police is the national lead force for online fraud and includes Action Fraud and the NFIB. Local policing is the responsibility of Police and Crime Commissioners and chief constables. From our interviews with key stakeholders and research by HM Inspectorate of Constabulary on digital crime in 2015, which covered six out of 43 forces, we found that forces may:

- have different approaches to reporting and recording fraud;
- not understand roles and responsibilities in relation to investigating fraud;
- provide poor advice and support to victims of fraud; and
- lack performance information around reporting and investigating fraud.

2.7 At the same time, the size of the police workforce has decreased every year since 2010, and in the year to 31 March 2016, fell by 3%. While traditional crime such as vehicle theft has also declined substantially, incidents of 'hidden' crimes recorded by the police, such as rape, the sexual exploitation of children, modern slavery, cyber crime and online fraud, are now known to be increasing (paragraph 1.6). These 'hidden' crimes can require new and different police responses. In 2016, nearly two million incidents of cyber-related fraud were estimated to have taken place, representing 16% of all estimated crime incidents. Faced with competing priorities for resources, Police and Crime Commissioners face a challenge in setting local priorities. Despite the level of economic crime, in 2016, one in six police officers' main function was neighbourhood policing, while less than one in 150 police officers' main function was economic crime.[21]

2.8 Online fraud 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. However, we found that only 27 out of 41 Police and Crime Commissioners referred to online fraud in their police and crime plans as at April 2017. The City of London Police provides quarterly information on fraud, which Commissioners should use to monitor and respond to fraud threats in their areas.

21 Home Office, *Police Workforce, England and Wales*, 31 March 2016: data tables, July 2016.

The response from the banking sector

2.9 Banks have an important role to play in protecting their customers against fraud. However, the protection banks provide varies, with some banks investing more than others in educating customers and improving their anti-fraud technology. A bank can refuse to refund all or part of an unauthorised payment if, for example, it considers that the customer failed to keep details of their banking password safe. In cases where customers have been scammed and voluntarily transferred money, banks often refuse to refund customers, and can do so legally, although banks may refund customers on a case by case basis. When a customer instructs their bank to transfer money from their account to someone else's account, these are known as push payments. Financial Fraud Action UK publishes fraud loss figures recorded by the UK's banks and card issuers. Some push payment fraud is included within the overall fraud loss figures, but it is not reported separately. Other data available on push payment fraud indicate that between 40% and 70% of people who are victims of scams do not get any money back. In January 2017, it was reported that a record 3,889 victims of romance fraud had lost £39 million in 2016, with some people losing up to £300,000 because of this type of fraud.[22] Banks are reported to be currently sitting on at least £130 million that cannot accurately be traced back and returned to victims.[23]

2.10 In September 2016, the consumer body Which? complained to the Payment Systems Regulator about banks failing to protect customers tricked into transferring money to a fraudster. Which? argued that shifting liability for scams onto banks would encourage them to protect their customers better. The Payment Systems Regulator concluded that there was not sufficient evidence to justify intervention at the time and that intervention would risk unintended consequences. The Payment Systems Regulator did find that the ways in which banks work together in responding to scams needed to improve, that some banks needed to do more to combat these types of scams, and that data available on the scale of these types of scam were poor. The Payment Systems Regulator announced it would be taking forward work with the Financial Conduct Authority and the banking industry. As part of this work, the Payment Systems Regulator agreed that the banking industry should lead on developing a common approach that payment service providers should follow when responding to instances of scams. The Payment Systems Regulator's work will look at whether payment systems operators can play an expanded role in minimising consumer harm caused by authorised push payment scams.[24]

2.11 However, some stakeholders hold an opposing view to that held by Which?. According to the Commissioner of the Metropolitan Police Service in 2016, banks should not refund victims if they fail to protect themselves.

22 BBC News, *Online dating fraud victim numbers at record high*, January 2017.
23 Payments Strategy Forum, A *Payments Strategy for the 21st Century: Putting the needs of users first: Supplementary documents,* November 2016.
24 Payment Systems Regulator, *Which? authorised push payments super-complaint: Payment Systems Regulator's response*, December 2016.

What the Department is doing to tackle online fraud

2.12 The Department has recognised that it cannot tackle online fraud on its own and needs to coordinate its approach with others. In February 2016, it launched the Joint Fraud Taskforce. The Taskforce comprises representatives from government, law enforcement and the banking sector to collaborate on tackling fraud, for example through sharing intelligence and making citizens and businesses more aware of the risk of fraud. **Figure 12** sets out the Taskforce's objectives, membership, governance and main strands of work. Oversight of the Taskforce is the responsibility of the Management Board and Oversight Board, chaired by the Home Secretary. There is no senior responsible owner.

2.13 The Taskforce's focus at this stage is primarily on banks, although parts of industry such as software companies, internet service providers, telecom companies and retailers can play a role in tackling the threat. In addition, the Taskforce focuses on the UK, although much fraud against victims in the UK is committed abroad.

2.14 Governance and accountability of online fraud presents a challenge to the Department, despite the creation of the Taskforce, for the following reasons:

- A large number of stakeholders play a role in preventing, reporting, disrupting and prosecuting the crime. Stakeholders include government bodies, the police, banks and private sector companies. All contribute in many different ways to decisions and policies.
- Organisations may not fulfil their responsibilities. For example, the government may be reluctant to legislate to reduce online fraud, while the private sector may be averse to accepting responsibility or liability for online fraud.
- Despite being set up in February 2016, the Taskforce has no clear success measures for its initiatives. Without clear indicators of the positive impact of the Taskforce, there is a risk that partners may be less willing to engage, especially since engagement relies on their goodwill.
- There are multiple issues to be addressed across technical, political, and economic areas, as Figure 12 shows.
- Since establishing the Taskforce, the Department has not published any information on its progress.
- There are no public data from the Department or industry on tackling, reducing and preventing online fraud.

2.15 We could not find any consistent reporting of fraud in major banks' annual reports and accounts, and there is no public information on losses incurred by individual banks, rather just an aggregate figure produced by Financial Fraud Action UK. Although membership of the organisation is voluntary, all Financial Fraud Action UK members, including all major retail banks and card issuers, are required to provide their individual fraud losses against an agreed set of reporting definitions and also their fraud prevention rates. These figures are validated by Financial Fraud Action UK.

Figure 12

The structure and work of the Joint Fraud Taskforce

The Taskforce is delivering a range of work to meet its objectives

Mission

Reduce the volume and impact of economic crime and the value of loss incurred, and to design out fraud.

Vision

1 Prevent more individuals and organisations from becoming victims of fraud.

2 Change consumer behaviour by communicating widely.

3 Protect the UK by making it a hostile environment for fraud.

Strategic objectives

Improve law enforcement's response to fraud.

Allow faster intelligence sharing.

Coordinate the work of law enforcement, government and banks.

Jointly assess threats and set priorities.

Deliver coordinated, innovative and long-lasting awareness campaigns.

Help develop initiatives to maximise support for fraud victims.

Reduce vulnerability by coordinating across different industries and organisations.

Identify and use technology to improve fraud detection and prevention.

Reduce legislative and regulatory barriers to effective fraud prevention.

Law enforcement	Raising awareness	Repatriating funds to victims	Tackling 'card not present' fraud	Victims and vulnerabilities
Lead				
Home Office and City of London Police	Home Office and Financial Fraud Action UK	Industry, reporting to Home Office	Industry, reporting to Home Office	British Bankers' Association and banks
Examples of work to support strategic objectives				
Develop a new data-sharing model, increase forces' prioritisation of fraud and roll out best practice so forces have suitable training.	Develop a visible, well-funded, and targeted prevention campaign, building on the 'Take Five' campaign.	Develop legislation and technology to help banks trace the movement of fraud funds through different bank accounts.	Establish minimum standards for authentication to reduce 'card not present' fraud.	Develop new bank accounts with opt-in safety features, for example to slow down payments, and train more bank branch staff to identify potential victims.

The Taskforce is delivering a range of work to meet its objectives

Oversight Board: Provides strategic direction, chaired by Secretary of State, meets twice a year.

Management Board: Chaired by Home Office, meets every eight weeks.

Members

Law enforcement	Industry	Fraud organisations and third sector
City of London Police	British Bankers Association	Cifas
National Crime Agency	Individual banks	Financial Fraud Action UK
Police and Crime Commissioners	Payment Services Forum	Victim Support
Regional Organised Crime Units	Merchants	
Local force representatives		
Trading Standards		

Source: Home Office

2.16 The Department, in leading the response to online fraud, has to influence Taskforce partners to take responsibility in the absence of more formal legal or contractual levers. The Department could learn from other examples of government working with the private or third sector to meet policy objectives. For example, in 2012 we reviewed the Compact, a voluntary agreement that set out shared principles for effective partnership working between the government and voluntary and civil society organisations in England. Our report set out a number of principles to support oversight of partnership working. These principles should be adapted and applied to the Department's oversight of the Taskforce. Leadership and ownership of the Taskforce should be supported by appropriate arrangements. Arrangements should support:

- internal and external reporting on the Taskforce's progress and implementation of initiatives;
- the promotion of the Taskforce, and the identification and dissemination of good practice to help improve performance;
- evaluation of the Taskforce's implementation of initiatives; and
- transparent relations with law enforcement and the private sector.

The principles described above should be:

- supported by relevant, evidence-based information;
- proportionate to the circumstances and minimise burden; and
- be assessed periodically to make sure they remain appropriate.[25]

25 National Audit Office, *Central government's implementation of the national Compact*, January 2012.

Part Three

Opportunities to improve the response

3.1 There are further opportunities to reduce online fraud by coordinating work across government, industry and law enforcement bodies on preventing, reporting, disrupting and prosecuting the crime. Although the Home Office (the Department) has work under way in all these areas, it considers its priority is preventing fraud, in line with its overall objective to prevent crime.

Prevention

3.2 To prevent online fraud, the government, working with others, wants to raise awareness of the crime and change people's behaviour. However, it also acknowledges government and industry have a duty to protect people from becoming victims.

Raise awareness and change people's behaviour

3.3 For online fraud, the traditional law enforcement response of tackling crime by pursuing criminals is not effective, as fraudsters are hard to trace and proceeds are rarely recovered. Instead, the Department and others must try to change the public's behaviour by raising awareness and educating citizens and businesses. In September 2016, Financial Fraud Action UK launched the Take Five campaign. Along with banks and other partners, it is providing initial funding of £1.4 million to the campaign until July 2017. The campaign will then receive further funding of £3.15 million from banks and the government to run up to 2018. The campaign is seeking to change people's behaviour so they protect themselves from scams better.

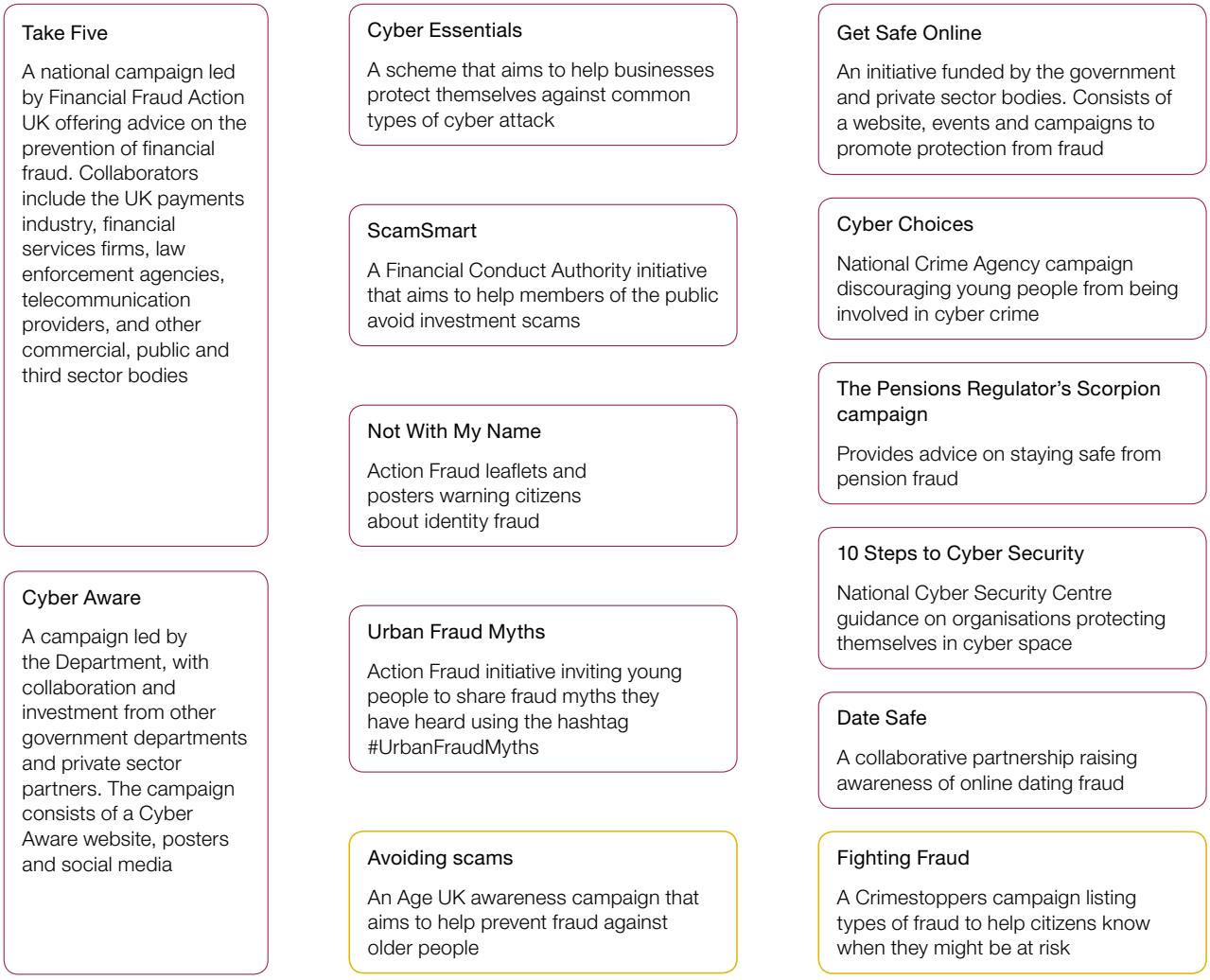
3.4 Stakeholders told us that the government has made some progress in recent years on working together across departmental and agency boundaries, and with industry and law enforcement agencies, to coordinate activities and messages about online fraud. However, there is often low awareness of these campaigns. As at 31 March 2017, we identified more than 10 campaigns backed by the government and others to educate citizens and businesses and raise awareness of cyber security (**Figure 13** overleaf). Too many competing campaigns from different organisations, often presenting slightly different messages, could confuse the public and limit impact.

3.5 Using different types of communication and messages is essential to engage different segments of the population. However, campaigns to raise awareness are often generic and not targeted at specific groups through different channels. This might include using social media for children and young people, and radio and print for older people.

Figure 13

Cyber security education and awareness campaigns as at 31 March 2017

Too many competitive campaigns from different organisations, often presenting slightly different messages, could confuse the public and reduce the impact of the campaigns



Source: National Audit Office analysis

3.6 It is difficult for the Department to measure the impact of the various campaigns and even more challenging to isolate the government's contribution to changing behaviours. There are opportunities for the Department, working with others, to do more, including:

- investing more in raising awareness through television, radio, digital and press advertising;
- targeting specific or more vulnerable groups, working with, for example, professional bodies representing lawyers and accountants, charities and banks' contact centres;
- ensuring a consistent message; and
- evaluating and measuring the success of public awareness campaigns.

3.7 The Department is already making progress in these areas. To make sure the Take Five campaign is better resourced and more 'joined-up', and has greater visibility and impact, the Department is providing an additional £0.5 million for an expanded version of the campaign, which is due to launch in the summer of 2017, with total additional funding of £3.15 million. The Department is also examining how it can measure the success of the Take Five campaign more effectively, although the results will not be available until March 2018.

Protect people at risk of becoming victims

3.8 Although educating people to stay safe online is sensible, the government, police and banks also have an important role in protecting people. As part of its wider responsibilities for national cyber security, the National Cyber Security Centre has a number of initiatives under way to protect people online, including around making email safer. For example, the Centre is seeking to stop spoof email and take down spoof websites, which can be used to commit online fraud. In addition, banks have a responsibility to keep customers' data secure so that it cannot be compromised by criminals and used to commit fraud.

3.9 There are also examples of good practice within local police forces, such as Sussex Police's Operation Signature. This initiative focuses on identifying victims and protecting vulnerable citizens from fraud by providing educational awareness videos to banks, community groups and people visiting the homes of vulnerable people. Internationally, an example of good practice is the Senior Support Unit within the Canadian Anti-Fraud Centre, which provides peer-to-peer support for vulnerable old people. However, it is not clear where forces and others can easily find and share good practice. There is an opportunity for the Department, or others, to identify, develop and share good practice in a more systematic way.

Reporting

3.10 Reporting and recording online fraud is important to:

- understand the scale, nature and risk of the crime;
- inform the development of government policy to reduce crime, and establish whether those policies are effective;
- build intelligence on crime to effectively respond and allow the police to prioritise investigations; and
- enable government and others to understand the level of resources needed for tackling the crime.

3.11 As set out in Part Two, effective analysis requires organisations to collect data and share information between themselves. However, as highlighted in Part One, there are significant gaps in data on the nature and scale of online fraud in the UK.

Collecting and analysing data

3.12 Action Fraud is the UK's national reporting centre for fraud and cyber crime. The National Fraud Intelligence Bureau (NFIB) analyses information from Action Fraud, and packages and shares it with police forces (Part Two). **Figure 14** sets out the process for reporting and recording fraud and shows that, at each stage of the process, cases can fall out of the system, and not be investigated or prosecuted. This 'attrition' can occur for a number of reasons. Citizens and businesses may:

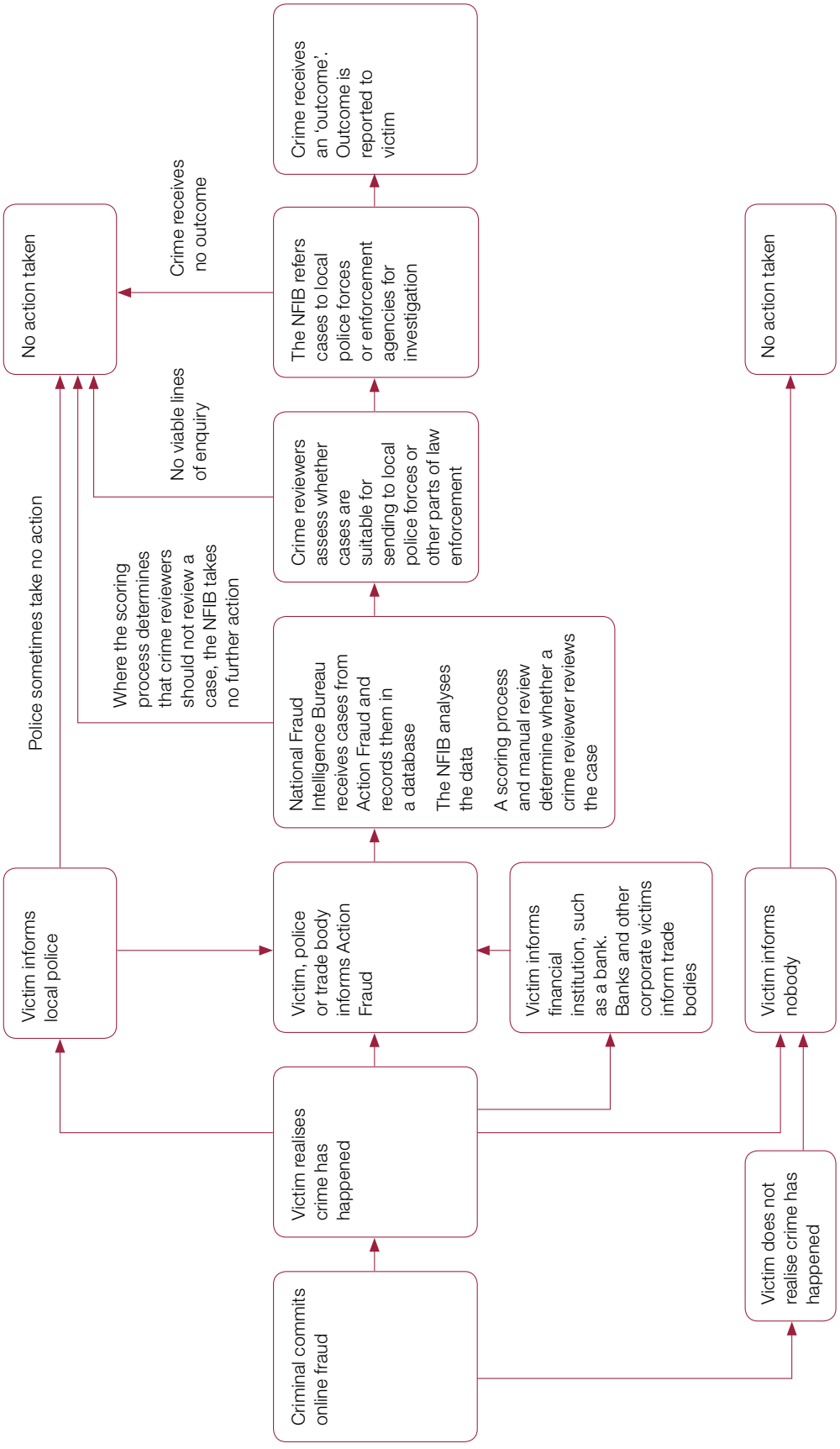
- not be aware of Action Fraud. For example, not all police forces' websites have a prominent and clearly visible link to Action Fraud from their home-pages; or
- not find it easy to report fraud, as the Action Fraud website is not user-friendly, although it has been redesigned and will be relaunched later in 2017.

Police forces may:

- not be aware of their responsibilities for reporting to Action Fraud, or report to Action Fraud in an inconsistent way. This includes referring victims straight to Action Fraud, when in fact the police should take a report from the victim and feed it into Action Fraud. There is no mandated process for how forces manage fraud reporting;
- not prioritise cases for investigation, or not investigate cases, as forces do not have sufficient skill and capacity and are not clear about how they should collaborate when cases cross force boundaries;
- have insufficient data recorded to identify offenders; or
- not always report outcomes to the NFIB.

Figure 14
The process for reporting and recording online fraud

At each stage of the process, cases can fall out of the system, and many cases may not be investigated or lead to a prosecution



Note

1 Citizens and businesses sometimes report cases to police or financial institutions.

Source: National Audit Office analysis

3.13 Action Fraud and the NFIB plan to introduce a new enhanced system for collecting and analysing data later in 2017 to help the government and others to improve their understanding of the threat. The new system will be more user-friendly and make it easier to report fraud. It should provide information to help forces prioritise fraud, and help the NFIB improve the information it passes on to the police, so that forces are better able to investigate cases. However, the success and impact of the new system, and its ability to support improved investigations and disruptions, will depend on the quantity and quality of the data it receives from citizens, businesses and industry. In addition, the National Cyber Security Centre aims to generate useful data to share with others through work on internet defence such as on the sources of spoof emails.

3.14 There is a lack of sharing of information between government, industry and law enforcement agencies on fraud. For example, there is no formal requirement for banks to report fraud or share reports with government.

Disruption

3.15 Disrupting fraud requires:

- developing capabilities to tackle fraud; and
- increasing the costs or reducing the benefits of crime.

Developing capabilities to tackle fraud

3.16 The government, financial institutions and telephone, email and internet service providers, among others, all have a role in disrupting online fraud. There are opportunities for them to work together to design out fraud. By way of example, the motor industry significantly reduced vehicle theft by improving vehicle security after the government published league tables of cars most at risk of being stolen.

3.17 The Department and banks recognise that there is no single solution, like Chip and PIN 10 years ago, to reduce online card fraud. As more people make payments online using cards, criminals have exploited this vulnerability by stealing card details and using them many times to transact online. The banks have plans to address this type of fraud by introducing cards that change their security code (the number on the back of the card) every hour. This is a positive step, as the re-design may help stop an increase in online card fraud. However, such a plan requires all card providers to participate. The Department will need to continue to work with industry to innovate as criminals find other ways to attack vulnerabilities. The Revised Payment Services Directive, new European legislation, aims to improve consumer protection against fraud from 2018 through enhanced security requirements, including the use of strong customer authentication for electronic payments. The Department told us that industry experts estimate these improvements could reduce ‘card not present’ fraud by 40%.

Increasing costs or reducing the benefits of crime

3.18 Fraudsters are increasing their use of social engineering to convince citizens to move their money into fraudsters' accounts, divulge credentials that enable fraudsters to move money out of victims' accounts, and purchase goods that do not exist. Technological advances in payment systems, such as faster payments, make it easier for fraudsters to receive and distribute fraud proceeds through multiple accounts at speed.

3.19 It is therefore difficult for banks to identify and stop funds, and return them to victims. The Joint Fraud Taskforce is currently testing the feasibility of a system to enable banks to do this more easily. To repatriate funds to victims, there will need to be participation from all banks and support from key stakeholders including HM Treasury, the Payment Systems Regulator, the Financial Conduct Authority and the Information Commissioner's Office.

Prosecution

3.20 To prosecute criminals effectively for online crime, it is important that effective legal powers are available; there is increasing cooperation with the international community.

Effective legal powers

3.21 The government wants to enable the police and encourage the judiciary to make greater use of existing laws in the UK to deal with online crime. Cases of online fraud can currently be prosecuted using the Computer Misuse Act (1990) or the Fraud Act (2006). In our interviews with stakeholders and literature review, many agreed it was possible to use existing laws to prosecute online fraud cases; however, government needs to ensure that current legislation remains applicable in the face of increasing technological change and rapidly evolving threats.

3.22 Although the prosecution rate for online fraud is low, there are limited data on the outcomes for fraud reports and investigations because data cannot easily be matched across the Department and the Ministry of Justice. Information on outcomes could help inform future investigations and prosecutions.

3.23 Sentencing guidelines for fraud take into account both the value of the fraud and the harm caused to the victim, particularly if the victim is considered vulnerable. However, according to some stakeholders, including the Department, criminals do not always receive sentences proportionate to the crime, in particular in relation to the non-financial harm victims suffer.

Improving international co-operation

3.24 Much online fraud is committed overseas. In 2016, the government's National Cyber Security Strategy reported that most serious cyber crime, including fraud, continued to be "perpetrated predominantly by financially motivated Russian-language organised criminal groups, with emerging threats from South Asia and West Africa".[26] Criminals often evade prosecution by being in countries where they will not face arrest.[27] From our interviews with law enforcement agencies and other stakeholders, it was evident that high-volume, low-value online fraud committed abroad against the UK is unlikely to be pursued, compared with domestic fraud or serious organised international fraud.

26 HM Government, *The UK Cyber Security Strategy 2011 to 2016*, Annual Report, April 2016.
27 Comptroller and Auditor General, *The UK cyber security strategy: Landscape review*, Session 2012-13, HC 890, National Audit Office, February 2013.

Appendix One

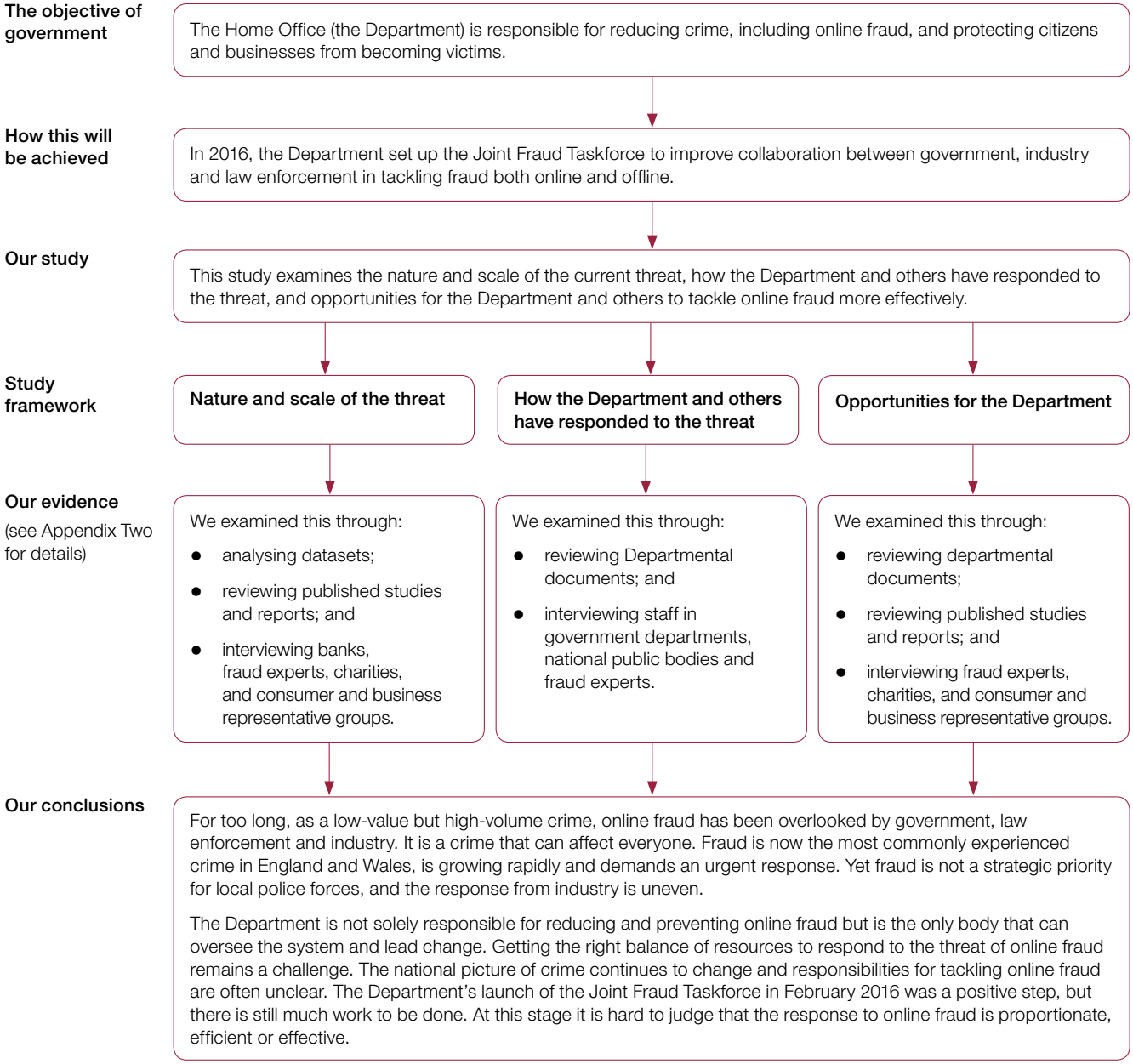
Our audit approach

1 The study examined the system for reporting and addressing online fraud used by public sector bodies to address online fraud committed against individuals and businesses. We assessed:

- the nature and scale of the threat;
- the government's response to the threat; and
- opportunities to improve the response.

2 **Figure 15** overleaf summarises our audit approach. Our evidence base is described in Appendix Two.

Figure 15
Our audit approach



Appendix Two

Our evidence base

1 We reached our independent conclusions on online fraud following our analysis of evidence collated between August 2016 and April 2017. Our audit approach is outlined in Appendix One.

2 We drew on a variety of evidence sources to examine the nature and scale of online fraud, how the Home Office and others have responded to the threat, and opportunities for the Department.

3 We conducted semi-structured interviews with key stakeholders.

Public sector organisations:

- Home Office.
- Cabinet Office.
- City of London Police.
- Department for Business, Energy & Industrial Strategy.
- Department for Communities & Local Government.
- Financial Conduct Authority.
- HM Inspectorate of Constabulary.
- National Crime Agency.
- National Cyber Security Centre.
- Payment Systems Regulator.
- Serious Fraud Office.

Other organisations:

- Age UK.
- Barclays.
- British Chamber of Commerce.
- British Retail Consortium.
- Centre for Counter-Fraud Studies, University of Portsmouth.
- Cifas.
- Financial Fraud Action UK.
- Fraud Advisory Panel.
- Lloyds Banking Group.
- TechUK.
- Victim Support.
- VocaLink.
- Which?

4 We analysed documents relating to the Joint Fraud Taskforce, including meeting minutes, risk registers and strategy documents. We also reviewed published and unpublished research and reports relating to online fraud and cyber security.

5 We carried out data analysis on a range of sources, including data from the Crime Survey for England and Wales, the Opinions and Lifestyle Survey, police recorded crime, Financial Fraud Action UK, the National Fraud Intelligence Bureau, Eurostat, the World Bank and Ofcom.

This report has been printed on Evolution Digital Satin and contains material sourced from responsibly managed and sustainable forests certified in accordance with the FSC (Forest Stewardship Council).

The wood pulp is totally recyclable and acid-free. Our printers also have full ISO 14001 environmental accreditation, which ensures that they have effective procedures in place to manage waste and practices that may affect the environment.

National Audit Office

Design and Production by NAO External Relations
DP Ref: 11473-001

£10.00

ISBN 978-1-78604-124-1