Office for National Statistics

Article

Nature of fraud and computer misuse in England and Wales: year ending March 2019

Summary of the various sources of data for fraud and computer misuse and what these tell us about victims, circumstances and long-term trends.

Contact:
Meghan Elkin
crimestatistics@ons.gov.uk
+44 (0)20 7592 8695

Release date:
19 March 2020

Next release:
To be announced

Table of contents

1 . Main points

The Crime Survey for England and Wales (CSEW) shows that there were an estimated 3.8 million incidents of fraud in the year ending March 2019, with evidence of a rising trend that is also seen in other data sources.

- While fraud victimisation showed little variation across different demographic groups, the likelihood of being a victim was generally lower in older age groups and greater in higher income households.
- In 63% of fraud incidents, there had been no contact between the victim and the offender; the most common methods of contact were online or by email (14%) or by telephone (11%).
- In 76% of fraud incidents, the victim incurred a financial loss and of these, the majority of victims (58%) lost less than £250.
- Around one in seven (15%) fraud incidents were reported to Action Fraud or the police; the most common reason given for not doing so was that the incident was reported to financial authorities instead.

The CSEW also showed there were an estimated 1.0 million incidents of computer misuse in the year ending March 2019, having fallen over each of the last two years.

- Around one in five (21%) computer virus incidents resulted in access to files or data being lost and in around one in eight (12%) incidents, a demand for money to release files or data was made.
- The majority of adults took precautions to keep safe online (for example, deleting suspicious emails without opening them) and the proportions of adults taking such precautions has risen.

2 . Defining fraud and computer misuse

Fraud involves a person dishonestly and deliberately deceiving a victim for personal gain of property or money or causing loss or risk of loss to another.

Most incidents fall under the legal definition of “Fraud by false representation”, where a person makes a representation that they know to be untrue or misleading at the time. This covers a broad range of fraudulent activity, with the most common types known to include:

- banking and payment card frauds
- consumer and retail frauds
- advance fee payment frauds

For more information on these types of fraud, see the Glossary.

Computer misuse covers computer viruses and any unauthorised access to computer material, as set out in the Computer Misuse Act 1990.

This is not limited to desktop or laptop computers, and it can include any device using operating software accessible online, for example: smartphones, games consoles and smart TVs. It includes offences such as:

- the spreading of viruses and other malicious software
- hacking or gaining unauthorised access to information
- denial-of-service (DoS) attacks (that is, the flooding of internet servers to disrupt or take down network infrastructure or websites)

Such crimes are encompassed within the wider concept of cyber crime (also referred to as online crime or cyber-dependent crime). Offences can be cyber-related but not classed as computer misuse (for example, online harassment via email or a social network account).

There are two principal sources of data currently used in the official statistics on fraud and computer misuse. The first is estimates from the Crime Survey for England and Wales (CSEW), a household victimisation survey. The second is incidents referred to the National Fraud Intelligence Bureau (NFIB) by Action Fraud (the national fraud and cyber crime reporting centre) as well as two industry bodies, Cifas and UK Finance, which report instances of fraud where their member organisations have been a victim.

For more information on these sources, including their strengths and limitations, see Quality and methodology.

3 . Trends in fraud

This article outlines recent trends in fraud and computer misuse. More up-to-date headline figures are published as part of the quarterly Crime in England and Wales bulletin.

Crime Survey for England and Wales (CSEW)

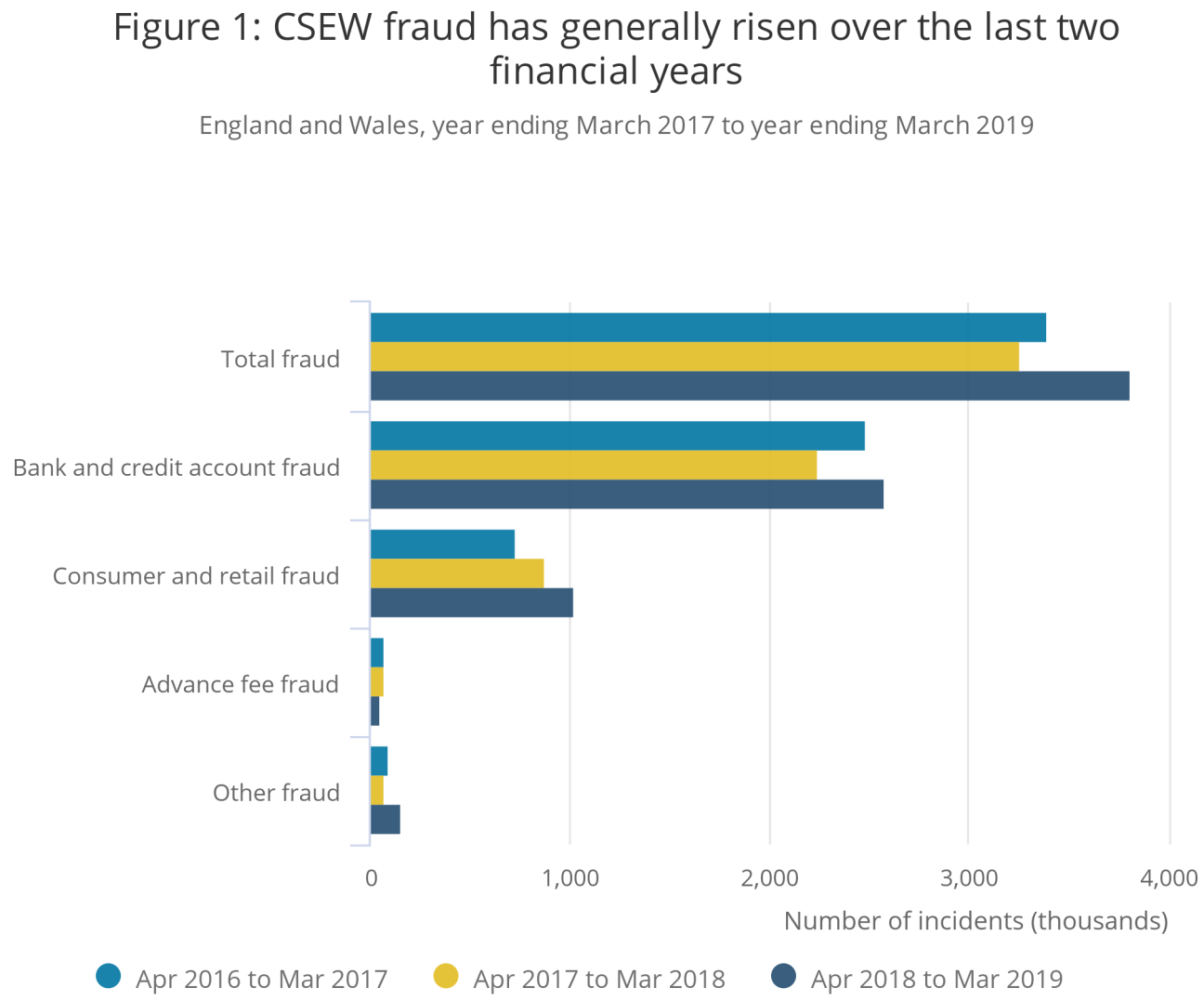
The CSEW shows evidence of a general increase in fraud incidents over the short time period where data are available (since the survey year ending March 2017). There were an estimated 3.8 million incidents of fraud in the year ending March 2019, accounting for around one-third (34%) of all CSEW crime estimated in this period. This was an increase of 17% from the previous year (3.3 million incidents) and an increase of 12% from the year ending March 2017 (3.4 million incidents) (Figure 1; Appendix table 1).

The increase has been caused by rises in consumer and retail fraud over the last two financial years and in bank and credit account fraud over the latest financial year.

Around half (54%) of fraud incidents in the year ending March 2019 were cyber-related. This is a similar proportion to the two preceding years.

Figure 1: CSEW fraud has generally risen over the last two financial years

England and Wales, year ending March 2017 to year ending March 2019



Source: Office for National Statistics – Crime Survey for England and Wales

Notes:

1. New victimisation questions on fraud and computer misuse were incorporated into the Crime Survey for England and Wales (CSEW) from October 2015. Up until September 2017, the questions were asked of half the survey sample. Since October 2017, the questions have been asked of a full survey sample.

2. In March 2018, the new CSEW estimates on fraud and computer misuse were assessed by the Office for Statistics Regulation against the Code of Practice for Statistics and were awarded National Statistics status.

National Fraud Intelligence Bureau (NFIB)

Data from the NFIB on fraud offences support the recent trend seen in the CSEW. This is seen in the steady increases in the total number of fraud offences referred to the NFIB in each year except for the year ending March 2018, which saw a small decrease of 2% (Figure 2).

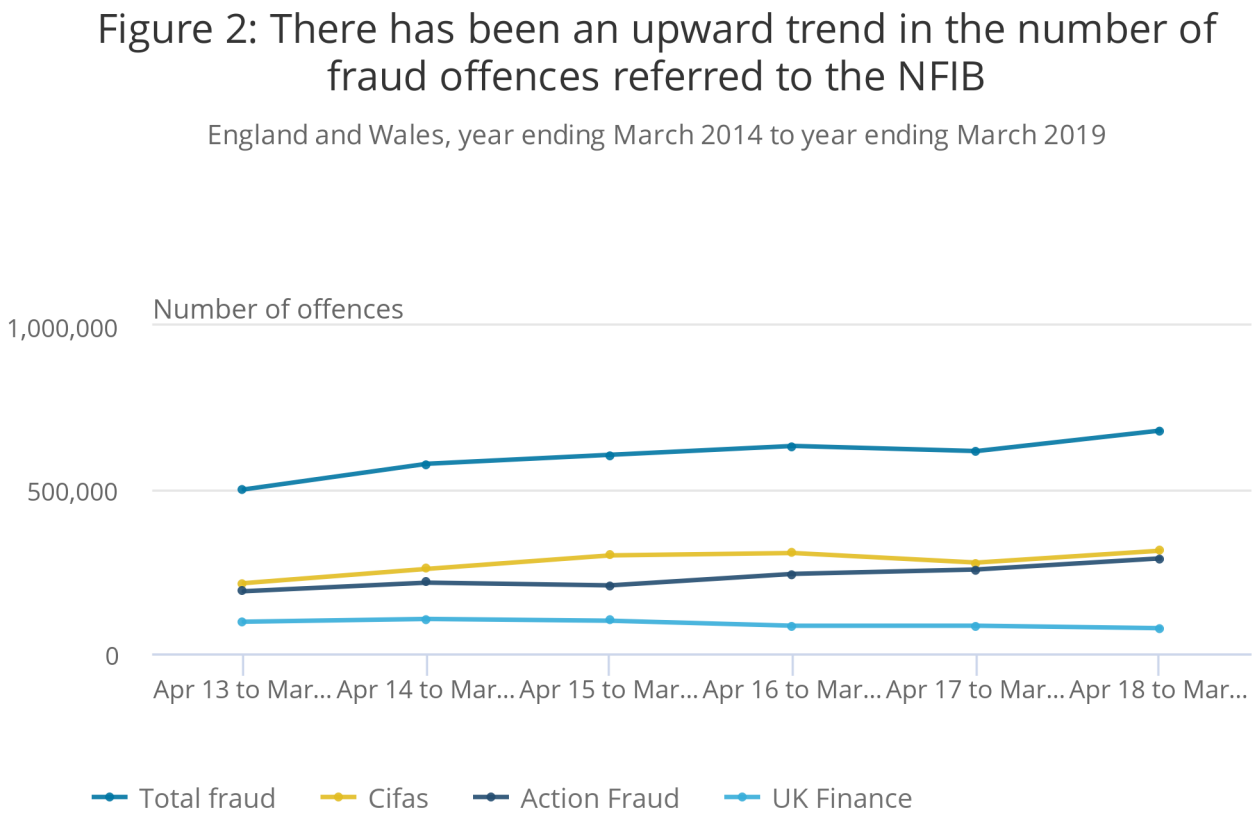
This trend has been caused by rises in the number of offences referred by Cifas and Action Fraud that have outweighed the falls in offences referred by UK Finance. [1]

UK Finance only refer cases to the NFIB where there is sufficient information to allow further investigation. Therefore, these data will not provide a complete reflection of all fraud that comes to their attention.

In the year ending March 2019, a total of 679,775 fraud offences were referred to the NFIB (Appendix table 3), accounting for around 11% of all offences recorded by the police or referred to the NFIB. This was an increase of 10% on the previous year (617,265 offences) and an increase of 36% compared with the year ending March 2014 (500,232 offences[2]).

Figure 2: There has been an upward trend in the number of fraud offences referred to the NFIB

England and Wales, year ending March 2014 to year ending March 2019



Source: Action Fraud and National Fraud Intelligence Bureau

Notes:

1. Fraud data are not designated as National Statistics.

2. Action Fraud did not record fraud offences across all England and Wales until April 2013. For trend analysis purposes, data for the years ending March 2012 and March 2013 have therefore not been presented.

3. Data for Action Fraud include an additional seven offences recorded by the police in the year ending March 2014.

4. In October 2018, Action Fraud launched a new fraud and cyber crime reporting service. The transition to the new system is not yet complete, and there has been a pause in the data feed from Cifas to the National Fraud Investigation Bureau (NFIB). Although fraud continues to be recorded by Cifas, cases from December 2018 have not yet been “referred” to the NFIB. Therefore, Cifas and NFIB figures for the year ending March 2019 are based on provisional data provided by Cifas. Once the issue has been resolved, the NFIB will hold a full copy of the data, allowing Cifas figures to be treated as confirmed and recognised as “referred” to the NFIB.

5. There may be some double or triple counting between Action Fraud, Cifas and UK Finance. Experts believe this duplication to be so small as to have an insignificant effect on crime trends, but there is currently no simple cross-referencing method within NFIB to detect the scale of it.

The number of incidents estimated by the CSEW is substantially higher than the number of incidents referred to the NFIB. This is because the survey captures a large volume of lower-harm cases that are less likely to have been reported to the authorities.

In contrast, incidents of fraud referred to the NFIB will mostly be focused on cases at the more serious end of the spectrum. These will only include crimes that are deemed serious enough to report to the authorities or where there are viable lines of investigation.

It is also important to note that owing to differences in coverage (the CSEW does not include offences against businesses), it is difficult to make meaningful comparisons between the two sources.

Additional UK Finance data

Additional data collected by UK Finance[3] provide a broader range of bank account and plastic card frauds than those referred for police investigation to the NFIB. These data also support the trends observed in both the NFIB data and the CSEW.

Over the last eight years, there has been a general rise in frauds (excluding push payments) involving UK-issued payment cards, remote banking and cheques reported by UK Finance.

There were 2.8 million such offences reported in the year ending March 2019. This is the fourth consecutive year-on-year increase, and the latest rise (39%) is the steepest year-on-year increase seen.

These data provide a better picture of the scale of bank account and plastic card fraud identified by financial institutions in the UK. More detailed information on these data can be found in Appendix table 4.

Notes for: Trends in fraud

1. It is important to note, particularly for Cifas and UK Finance, that trends will be influenced by referral practices.

2. Includes seven offences recorded by the police during this period.

3. Data sourced via their CAMIS system, which contains cases where it has been judged that there is no evidential value and no realistic chance of identifying the offender. CAMIS data also include those cases referred by UK Finance to the NFIB.

4 . Trends in computer misuse

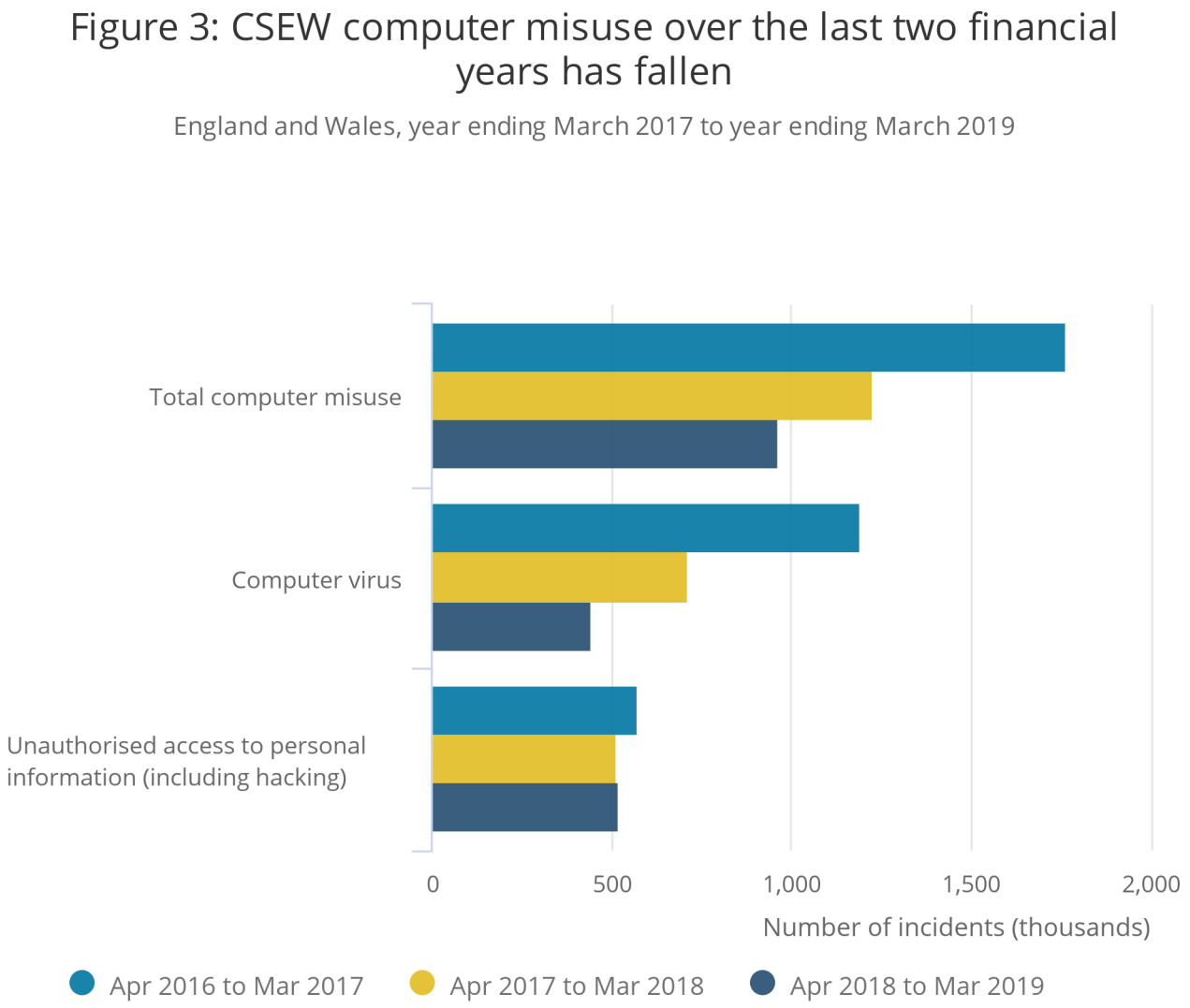
Crime Survey for England and Wales (CSEW)

The CSEW shows evidence of falls in computer misuse incidents over the short time period where data are available (since the survey year ending March 2017). There were an estimated 1.0 million incidents of computer misuse in the year ending March 2019. This was a decrease of 21% from the previous year (1.2 million incidents) and a decrease of 45% from the year ending March 2017 (1.8 million incidents) (Figure 3; Appendix table 2).

These decreases have been driven by falls in computer viruses over the last two financial years. Incidents of unauthorised access to personal information (including hacking) have remained stable over this period.

Figure 3: CSEW computer misuse over the last two financial years has fallen

England and Wales, year ending March 2017 to year ending March 2019



Source: Office for National Statistics – Crime Survey for England and Wales

Notes:

1. New victimisation questions on fraud and computer misuse were incorporated into the Crime Survey for England and Wales (CSEW) from October 2015. Up until September 2017, the questions were asked of half the survey sample. Since October 2017, the questions have been asked of a full survey sample.

2. In March 2018, the new CSEW estimates on fraud and computer misuse were assessed by the Office for Statistics Regulation against the Code of Practice for Statistics and were awarded National Statistics status.

Action Fraud

In contrast to the CSEW, data from Action Fraud suggest an increase in overall computer misuse offences in recent years.

Action Fraud (which receives reports from both individuals and businesses) recorded a total of 21,322 computer misuse offences in the year ending March 2019. This was an increase of 1% on the previous year (21,093 offences) and the third consecutive year-on-year increase (Figure 4; Appendix table 3). However, the number of offences in the latest financial year was 2% less than the peak number recorded by Action Fraud in a financial year (year ending March 2014; 21,686 offences).

We believe an increasing awareness of falling victim to hacking, leading to a greater likelihood of incidents being reported, has contributed to the overall rise. Computer misuse crimes such as extortion hacking are more likely to target companies (than individuals or households). As these are not captured by the CSEW, it is not surprising to see a different trend between the two data sources.

Despite the overall increase in computer misuse offences in the year ending March 2019, computer viruses (4,177 offences) have decreased by 42% since the year ending March 2017 (7,249 offences), mirroring the trend seen in the CSEW.

Figure 4: Computer misuse offences recorded by Action Fraud rose for the third consecutive year

England and Wales, year ending March 2013 to year ending March 2019

Source: Action Fraud, National Fraud Intelligence Bureau

Notes:

1. Computer misuse data are not designated as National Statistics.

2. Action Fraud did not start recording computer misuse offences until January 2012. For trend analysis purposes, data for the year ending March 2012 have therefore not been presented.

As with fraud, the number of computer misuse incidents estimated by the CSEW is substantially greater than the number of incidents referred to the National Fraud Intelligence Bureau (NFIB). This is owing to the extremely low proportion of computer misuse offences that are reported to the authorities. As such, computer misuse incidents referred to the NFIB provide a better indication of the demand on law enforcement rather than a good measurement of the prevalence of computer misuse.

5 . Fraud: characteristics of victims

Unlike many other types of crime, fraud, by its nature, is often committed anonymously, with the offender not having a specific target in mind. As such, there tends to be considerably less variation in fraud victimisation rates across different demographic groups than with other crime types. For example, there is no statistically significant difference in the likelihood of men or women being victims.

However, over the last three financial years (up to the survey year ending March 2019), some demographic groups have been consistently more or less likely to be victims of fraud according to the Crime Survey for England and Wales (CSEW).

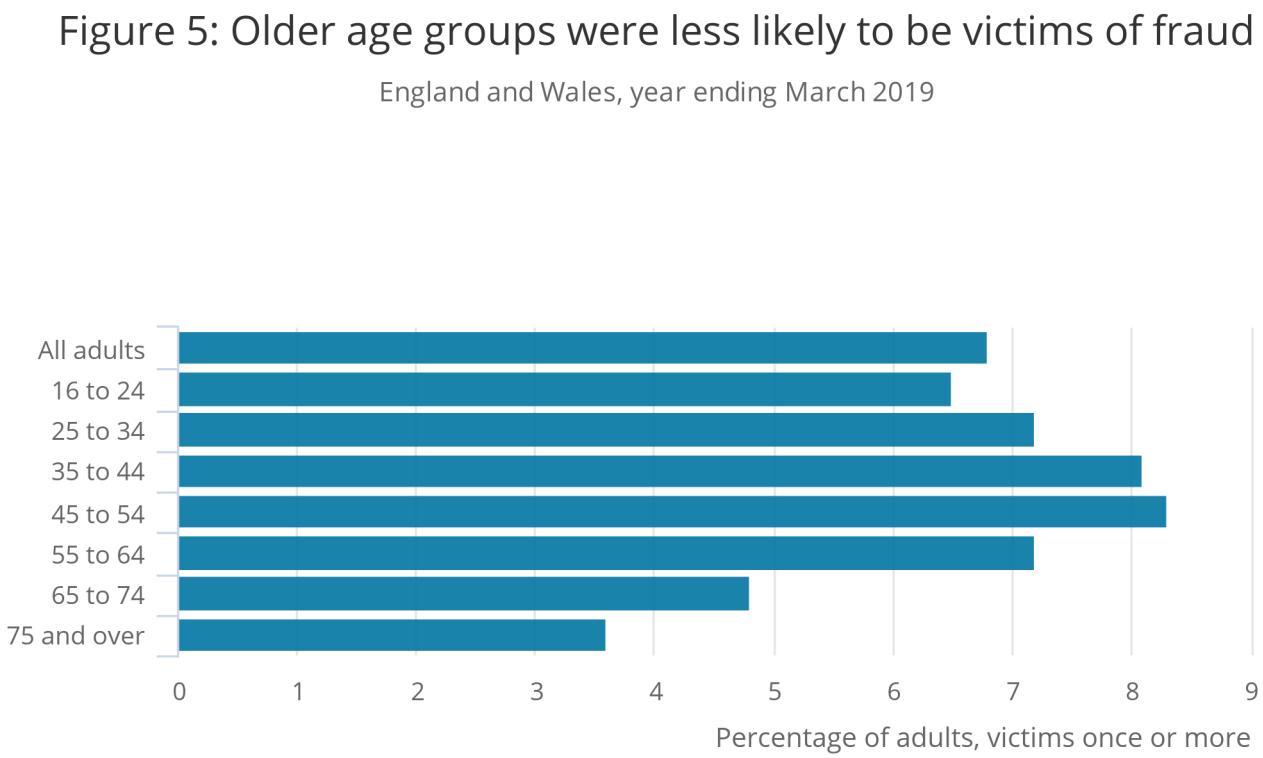
Age

As with other crime types, adults aged 65 years and over were less likely to be a victim of fraud than those in younger age groups. An estimated 4.8% of adults aged 65 to 74 years and 3.6% of adults aged 75 years and over were victims of fraud in the year ending March 2019, compared with 6.5% and above for all other age groups (Figure 5, Appendix table 7). Unlike other crime types, though, there is little variation in victimisation rates across other age groups (adults aged 16 to 64).

Lower victimisation rates in older age groups may appear contrary to other reports on victims of fraud, where it is often reported that older people are more vulnerable to becoming victims. However, the types of fraud where evidence suggests that older people are more likely to be victims, such as lottery scams and investment frauds, represent only a small proportion of CSEW fraud.

Figure 5: Older age groups were less likely to be victims of fraud

England and Wales, year ending March 2019



Source: Office for National Statistics – Crime Survey for England and Wales

Household income

Adults living in higher income households (that is, those earning £50,000 or more) tended to be the most likely victims of fraud (8.2% in the year ending March 2018) (Property crime table 11, year ending March 2018).[1] Household income is likely to be highly correlated with educational qualifications and occupation. For example, adults with university degrees or diplomas and adults working in managerial and professional occupations also tended to show higher rates of victimisation.

Geographic region

Additionally, the year ending March 2019 CSEW suggests that adults resident in the North East (3.6%) were the least likely to be victims of fraud. Adults resident in the East of England (8.3%), the South East (7.9%) and London (7.9%) were the most likely[2] to be victims (Appendix table 8).

This pattern is consistent with the data available from Action Fraud that indicate the North East (3 per 1,000 population) had the lowest rate of recorded fraud offences[3]. London, the East of England and the South East (all 5 per 1,000 population) had the three highest rates in the year ending March 2019 (Appendix table 5).

Repeat victimisation

Around one in eight (13%) victims of fraud in the year ending March 2019 were victimised more than once (Appendix table 6). This proportion has remained fairly constant in the three years for which data are available. It is lower than for victims of violence (25%) and criminal damage (19%) but around the same as for victims of domestic burglary and vehicle-related theft (both 12%).

For more data on repeat victimisation, see Annual trend and demographic tables D7 and D9.

Notes for: Fraud: characteristics of victims

1. Data relate to the year ending March 2018 as household income was not asked in the year ending March 2019 CSEW.

2. Not statistically significantly higher than all other regions.

3. The Action Fraud geographical data include computer misuse offences (in addition to fraud offences). However, these constitute only a small proportion of all reported offences and, thus, are unlikely to affect the distribution to any meaningful extent.

6 . Fraud: contact between victim and offender(s)

In almost two-thirds (63%) of incidents in the year ending March 2019 Crime Survey for England and Wales (CSEW), there had been no contact between the offender and the victim (Nature of crime: fraud and computer misuse table 5).

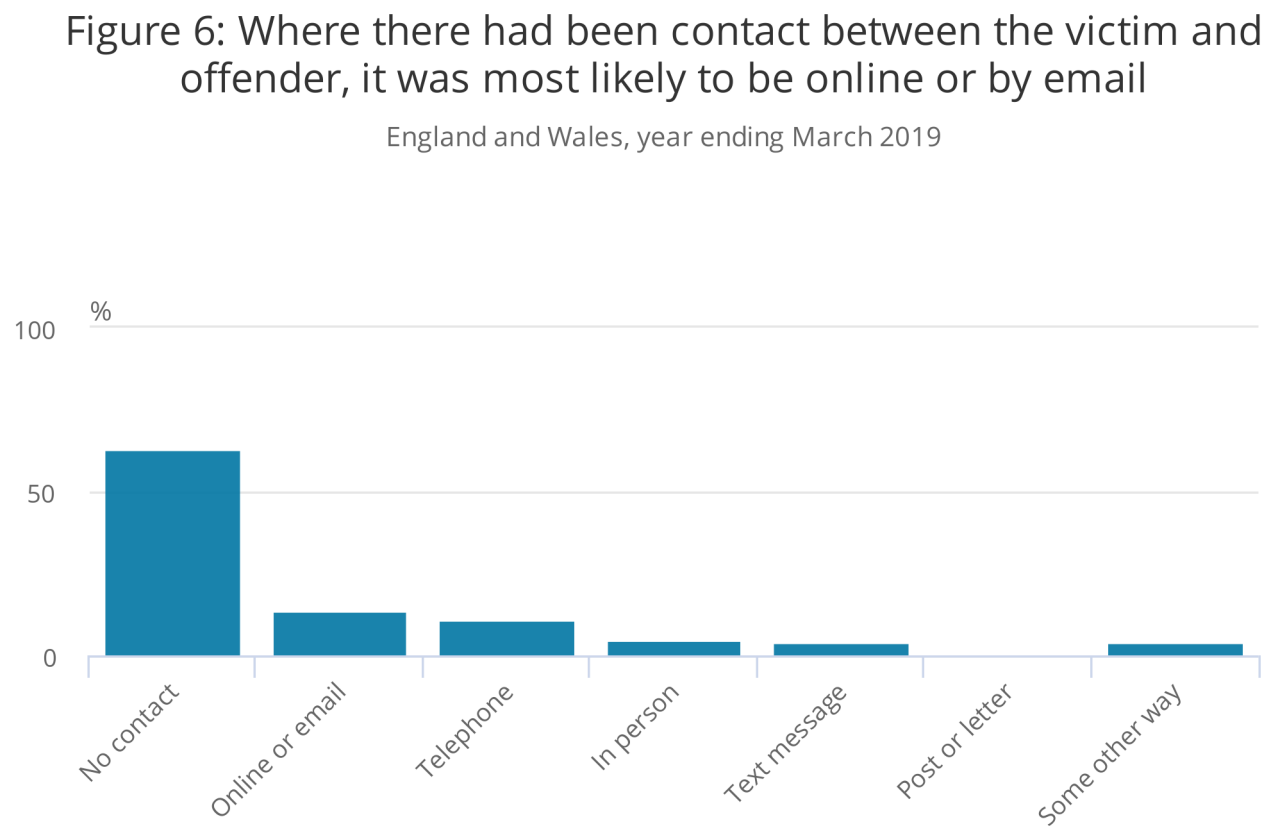
This varies for different types of fraud, with the proportion of incidents where there was no contact substantially higher for bank and credit account fraud (77%) compared with consumer and retail fraud (32%) and "all other fraud" (36%). The higher proportion for bank and credit account fraud is likely to reflect the different nature of these crimes. In many instances, victims find that money has been taken out of their account without their prior knowledge and no contact with the victim was required by the offender to commit the offence.

First method of contact

In the year ending March 2019, the most common first method of contact between the offender and the victim was online or email (14%). A further 11% of first contacts were by telephone, 5% were in person and 4% were by text message (Figure 6).

Figure 6: Where there had been contact between the victim and offender, it was most likely to be online or by email

England and Wales, year ending March 2019



Source: Office for National Statistics – Crime Survey for England and Wales

Notes:

1. Figures may not sum to 100 as more than one response is possible.

Reason for first contact

Where there was contact between the offender and the victim, the most common reason for contact in the year ending March 2019 was regarding buying or selling items online (18%). Other common reasons included unsolicited help to repair a computer or laptop (7%) and selling bogus services (5%) (Nature of crime: fraud and computer misuse table 6).

Offender details

In the year ending March 2019, around one in six (18%) of adults who were victims of fraud were able to say something about the offender(s). This proportion was not significantly different to that seen in the two previous years (both 17%) (Nature of crime: fraud and computer misuse table 7).

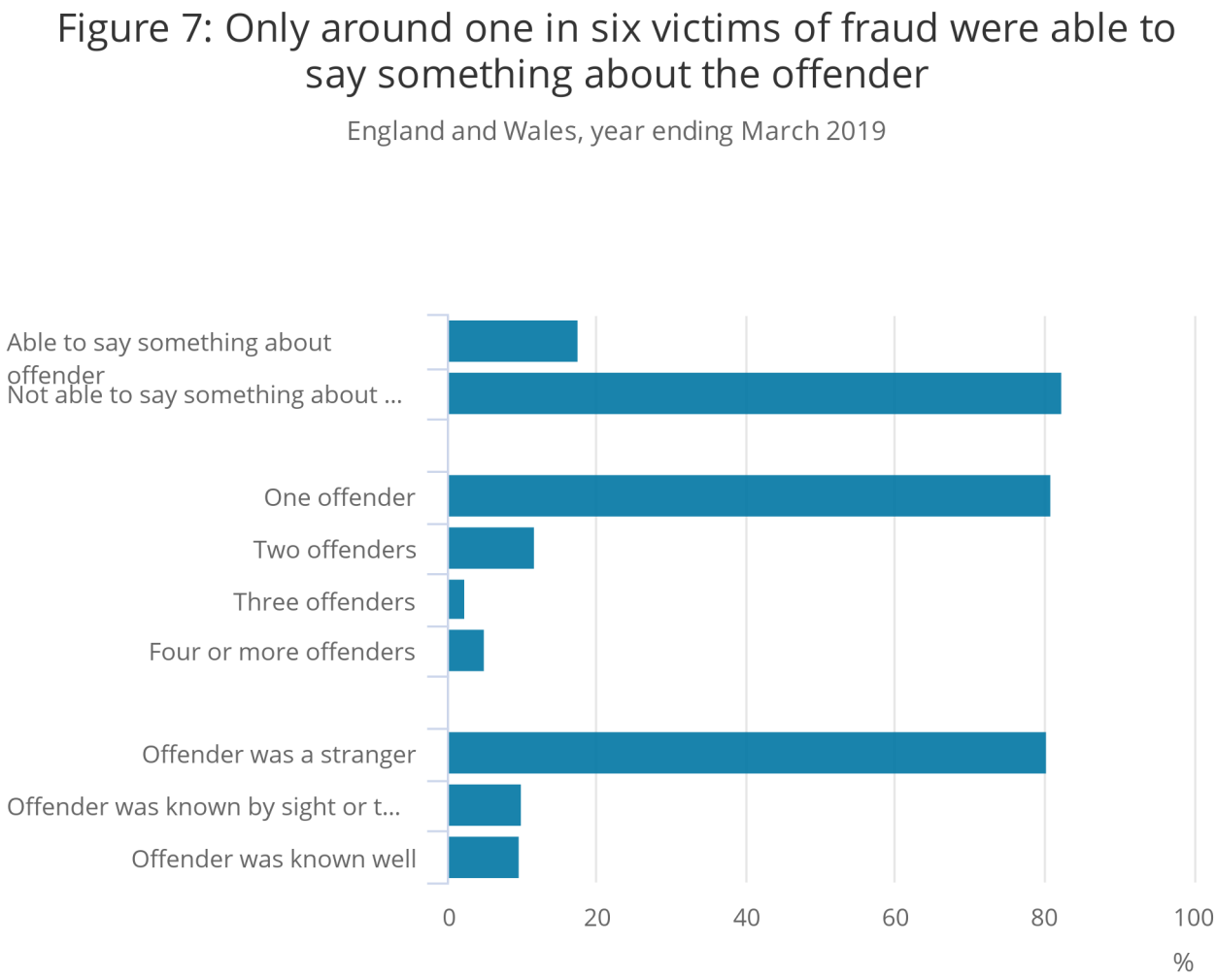
This proportion varied considerably across the different fraud types. The victim was able to say something about the offender in:

- around one-tenth (9%) of bank and credit account frauds
- around one-third (35%) of consumer and retail frauds
- just under half (45%) of “all other fraud” incidents

In these cases, the victim reported there being only one offender in around four in five (81%) fraud incidents. The offender was unknown to them also in around four in five incidents (80%) (Figure 7).

Figure 7: Only around one in six victims of fraud were able to say something about the offender

England and Wales, year ending March 2019



Source: Office for National Statistics – Crime Survey for England and Wales

Notes:

1. The percentages for whether the victim was able to say something about the offender relate to all victims. The percentages for number of offenders and relationship between the victim and the offender relate to victims who were able to say something about the offender.

2. The offender–victim relationship is classified as: “stranger”, if the victim did not have any information about the offender(s) or did not know and had never seen the offender(s) before; “known by sight or to speak to”, if at least one offender falls into either category; and “known well”, if at least one offender falls into this category (for multiple offenders, this takes priority over any less well-known offenders).

While the proportion of incidents in which the victim reported there being only one offender was similar across fraud types (all at around four in five), the relationship between the offender and the victim for consumer and retail frauds showed a different pattern to the other fraud types.

In 7% of incidents of consumer and retail fraud where the victim was able to say something about the offender, the offender was known (either well, by sight or to speak to) to the victim. In contrast, in around a third of instances of both “all other fraud” (32%) and bank and credit account fraud (34%), the offender was known to the victim. In the latter case, given the small proportion of bank and credit account frauds where the victim was able to say something about the offender, this represents only a small proportion of all bank and credit account frauds (3%).

7 . Fraud: amount and type of loss incurred

Amount of financial loss

Fraud victims did not incur any financial loss in around one in four (24%) incidents in the year ending March 2019 Crime Survey for England and Wales (CSEW). This was a lower proportion than the previous year and the year ending March 2017 (both 30%) (Nature of crime: fraud and computer misuse table 8).

In incidents for which victims suffered a financial loss[1] in the year ending March 2019 (Figure 8):

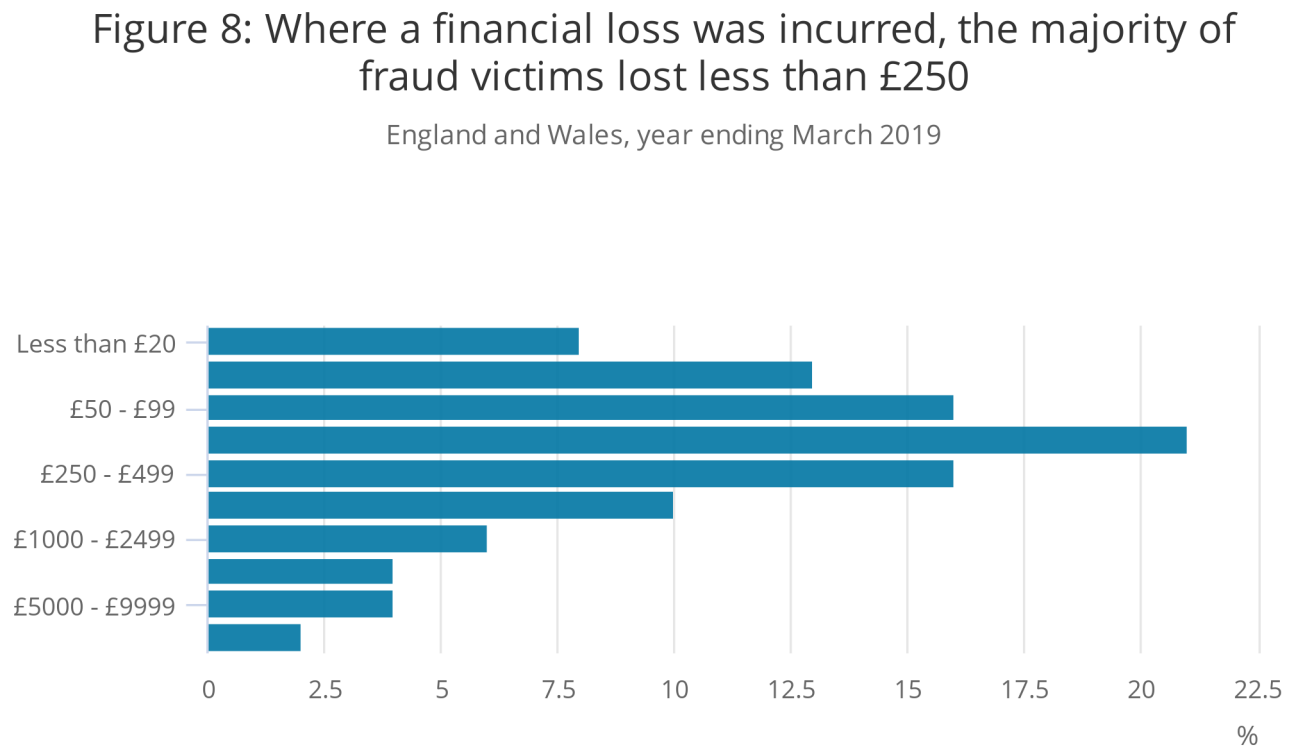
- the majority (58%) incurred a loss of less than £250, with the median loss being £167
- around a quarter (27%) incurred a loss of between £250 and £999
- the remainder (15%) incurred a loss of £1,000 or more, with 2% losing £10,000 or more

A broadly similar pattern was seen when looking specifically at bank and credit account fraud or consumer and retail fraud.

The CSEW, however, does not capture frauds against businesses or higher-harm or higher-loss incidents of fraud well, given their greater rarity. As such, while CSEW data give a good indication of financial loss incurred in the most commonly occurring frauds, they do not provide a good measure of overall loss as a result of fraud.

Figure 8: Where a financial loss was incurred, the majority of fraud victims lost less than £250

England and Wales, year ending March 2019



Source: Office for National Statistics – Crime Survey for England and Wales

Notes:

1. Financial loss represents incidents where an amount of money or cash had been stolen or taken as a direct result of fraud, regardless of any later reimbursement, or any additional charges or costs incurred (such as bank charges, repair costs or replacement costs).

Reimbursement

For incidents where the victim suffered a financial loss, the victim was fully reimbursed in around three-quarters (76%) of incidents (Appendix table 11). This proportion varies considerably across the different fraud types. Victims were fully reimbursed in:

- 88% of incidents of bank and credit account fraud
- 47% of incidents of consumer and retail fraud
- 33% of "all other fraud" incidents

How money was lost

In many cases, data are not collected by the CSEW on how money was lost. This is because victims had either not been in contact with the offender or, where contact had been made, the victim did not engage with the offender. However, for victims who did respond to fraudulent communication, information is available on how they lost money (Nature of crime: fraud and computer misuse table 9).

Around half (53%) of fraud victims responded to fraudulent communication they received. Of victims who responded to the fraudulent communication[2], 43% incurred a loss by giving, sending or transferring money.

The remaining 57% of those who responded to fraudulent communication either incurred a loss with the money having been taken by the offender without the victim's consent (as opposed to being provided by the victim) or did not actually incur a loss.

In cases where money was transferred, this was via:

- a "push payment" method in around 6 in 10 (59%) incidents
- a "pull payment" method in around 1 in 10 (10%) incidents
- a combination of using push and pull payment methods in fewer than 1% of incidents
- an unknown[3] method in the remaining 31% of incidents

See the Glossary for definitions of push and pull payments.

How fraud was discovered

There were two common methods in which victims first discovered they had experienced fraud in the year ending March 2019 (Nature of crime: fraud and computer misuse table 10). Around 4 in 10 (40%) victims saw an unrecognised transaction on a financial statement or found money missing from an account themselves. A further 3 in 10 (31%) victims were directly contacted or told by a financial institution (bank, building society or credit card company).

Notes for: Fraud: amount and type of loss incurred

1. Financial loss represents incidents where an amount of money or cash had been stolen or taken as a direct result of fraud, regardless of any later reimbursement or any additional charges or costs incurred (such as bank charges, repair costs or replacement costs).
2. Includes victims who did not know or could not remember if they responded.
3. After questions on payment methods had already been asked (though only to those who previously indicated that they transferred money to the offender), victims later clarified that money had been sent to the offender but they were not subsequently asked about payment methods. "Unknown" also includes victims who answered "Other" (or "None of these") to the question on how money had been transferred, but with no further information being available.

8 . Fraud: impact on victims

Emotional impact

In 78% of fraud incidents in the year ending March 2019 Crime Survey for England and Wales (CSEW), the victim was emotionally affected in some way. This proportion was up from 73% in the previous year and 71% in the year ending March 2017 (Nature of crime: fraud and computer misuse table 1).

Victims were “very much affected” in 10% of fraud incidents in the year ending March 2019. Typically, this proportion is lower than for incidents of burglary, violence and robbery and around the same level as that for vehicle-related theft and theft of personal property.

Across the fraud types, victims were less likely to be “very much affected” by incidents of bank and credit account fraud (9%) and consumer and retail fraud (11%) than “all other fraud” (21%) (Figure 9).

Figure 9: Victims of fraud were most likely to be very much affected by “all other fraud”

England and Wales, year ending March 2019

Source: Office for National Statistics – Crime Survey for England and Wales

Notes:

1. “All other fraud” refers to advance fee fraud and other fraud combined.

The most common forms of emotional reaction to fraud incidents in the year ending March 2019 were annoyance (70%), anger (49%) and shock (30%). Smaller proportions of victims experienced more serious emotional reactions, such as anxiety or panic attacks (9%), fear (8%) and depression (4%).

Other impact

In addition to emotional impact, the CSEW also asks respondents about other impacts on them as a result of being a victim of fraud (Nature of crime: fraud and computer misuse table 2).

Victims indicated they were impacted by financial loss[1] in 30% of fraud incidents and by loss of time or inconvenience in 24% of incidents in the year ending March 2019.

In 45% of all fraud incidents, the victim claimed they were not impacted at all. This proportion varies slightly across fraud types:

- 49% of bank and credit account frauds
- 41% of “all other frauds”
- 36% of consumer and retail frauds

The higher proportion of victims not impacted by bank and credit account fraud could be linked to the considerably higher proportion of these incidents in which the victim was fully reimbursed for their financial loss.

Notes for: Fraud: impact on victims

1. This estimate of financial loss is not comparable with the estimate presented in Section 7 as it is likely that victims will not have considered themselves impacted by a financial loss in instances where they were fully reimbursed.

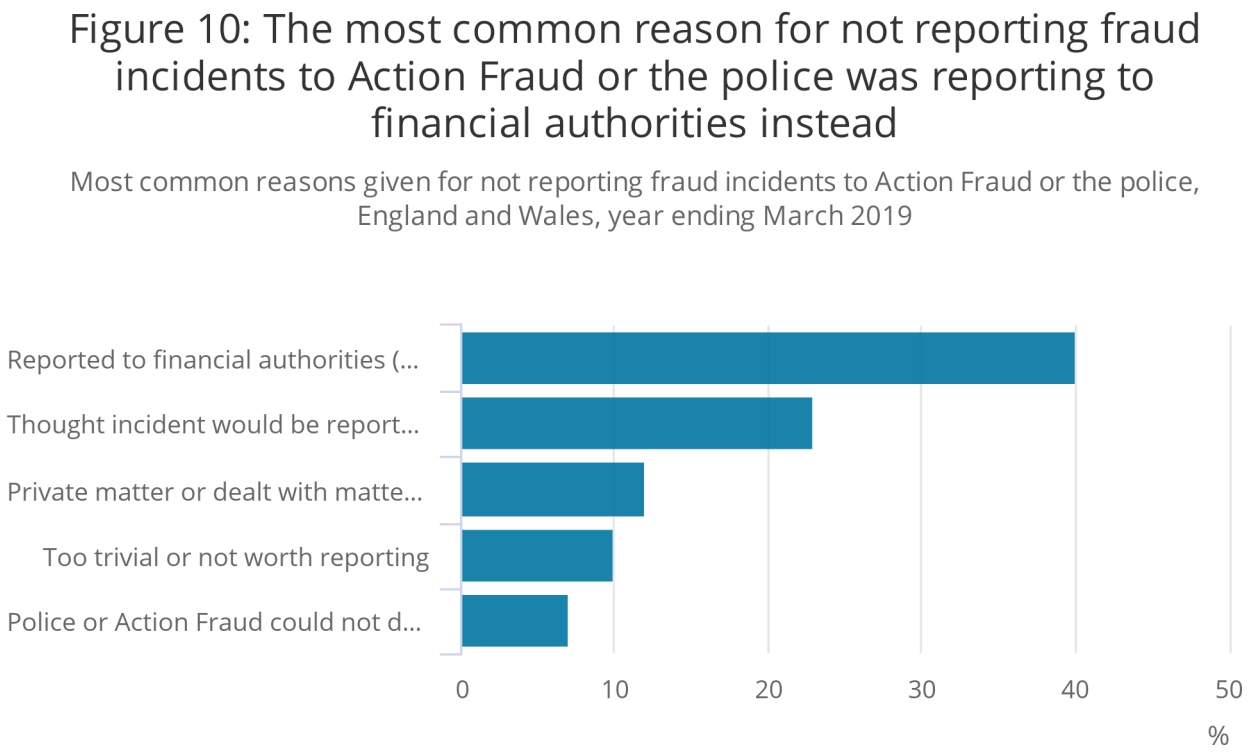
9 . Fraud: reporting to Action Fraud

In the year ending March 2019 Crime Survey for England and Wales (CSEW), around one in seven (15%) fraud incidents were reported to Action Fraud or the police (Appendix table 12).[1] Other than computer misuse (of which 6% of incidents were reported), this was the lowest rate of reporting across all headline crime types.

Among reasons why victims did not report fraud incidents to Action Fraud or the police, the most common was that the incident was reported to financial authorities (40%) (Figure 10; Appendix table 13). Other common reasons for victims not reporting included that it was thought that the incident would be reported by another authority (23%), it was a private matter or dealt with themselves (12%), and the incident was too trivial or not worth reporting (10%).

Figure 10: The most common reason for not reporting fraud incidents to Action Fraud or the police was reporting to financial authorities instead

Most common reasons given for not reporting fraud incidents to Action Fraud or the police, England and Wales, year ending March 2019



Source: Office for National Statistics – Crime Survey for England and Wales

Separate data indicated that in the year ending March 2019, around one in four (22%) fraud victims had heard of Action Fraud prior to their interview (data not shown).

Around 1 in 10 (10%) fraud incidents in the year ending March 2019 were reported directly to Action Fraud (Nature of crime: fraud and computer misuse table 11). This proportion was not significantly different to that seen in the two previous years.

Of fraud incidents reported, victims were very satisfied with how Action Fraud handled the incident in 24% of cases. This proportion was lower than the 38% of incidents reported in the year ending March 2017 (Figure 11; Nature of crime: fraud and computer misuse table 11). Victims were a bit dissatisfied with the handling of their incident in 18% of cases and very dissatisfied in 21% of incidents. Both of these proportions were higher than in the year ending March 2017 (7% and 10% respectively).

Figure 11: Victims were less satisfied with Action Fraud's handling of reported fraud incidents than two years ago

England and Wales, year ending March 2017 and year ending March 2019

Source: Office for National Statistics – Crime Survey for England and Wales

Notes for: Fraud: reporting to Action Fraud

1. Victims of fraud should report incidents to Action Fraud, rather than the police. If incidents are reported to the police, victims will be referred to Action Fraud (though they may choose not to subsequently report to Action Fraud).

10 . Nature of computer misuse

Characteristics of victims

As with fraud, by its nature, computer misuse offences are often committed anonymously, with the offender not having a specific target in mind. As such, there tends to be considerably less variation in computer misuse victimisation rates across different demographic groups than with other crime types.

However, over the last three financial years (up to the survey year ending March 2019), some demographic groups have been consistently more or less likely to be victims of fraud according to the Crime Survey for England and Wales (CSEW).

Adults aged 75 years and over were less likely to be a victim of computer misuse than those in younger age groups. An estimated 0.8% of adults aged 75 years and over were victims of computer misuse in the year ending March 2019, compared with 1.6% and above for all other age groups (Appendix table 9). This is likely to be related to lower ownership (and usage) of internet-enabled devices among those in older age groups. [1]

Men were more likely to be victims of computer misuse than women. An estimated 2.0% of men were victims of computer misuse in the year ending March 2019, compared with 1.6% of women.

Emotional impact

In 68% of computer misuse incidents in the year ending March 2019, the victim was emotionally affected. This proportion was not significantly different to that seen in the previous two years. (Nature of crime: fraud and computer misuse table 1).

A greater proportion of victims were emotionally affected by experiencing a computer virus (74%) than unauthorised access to personal information, including hacking (63%).

The most common forms of emotional reaction to computer misuse incidents in the year ending March 2019 were annoyance (77%) and anger (34%). Smaller proportions of victims experienced more serious emotional reactions, such as fear (10%), anxiety or panic attacks (7%), and depression (2%).

Other impact

Victims indicated they were impacted by loss of time or inconvenience in 30% of computer misuse incidents and by financial loss in 15% of incidents in the year ending March 2019 (Nature of crime: fraud and computer misuse table 2).

In 55% of all computer misuse incidents, the victim claimed they were not impacted at all. However, this proportion varies considerably between the two computer misuse types: unauthorised access to personal information including hacking (68%) and computer virus (40%).

Type of device affected by computer virus

In 9 in 10 computer virus incidents (91%), the device affected was a computer (63% a laptop or netbook computer and 28% a desktop computer). Other devices affected included mobile phones (5%) and tablets or iPads (4%) (Nature of crime: fraud and computer misuse table 12).

Experiences with computer viruses

For victims of computer viruses in the year ending March 2019:

- in 37% of incidents, the victim thought the virus was a direct result of opening an email, attachment or weblink that they received
- in 37% of incidents, the victim thought the virus was not a direct result of opening an email, attachment or weblink that they received
- in the remaining 25% of incidents, the victim did not know how the computer virus infected their device (Nature of crime: fraud and computer misuse table 13)

The two most common effects on virus-infected devices were that the device performed badly or stopped working (62% of incidents) and pop-ups were constantly appearing on screen (33% of incidents). Around one in five (21%) incidents resulted in access to files or data being lost and in around one in eight (12%) incidents, a demand for money to release files or data was made.

Notes for: Nature of computer misuse

1. See Internet users, UK: 2019.

11 . Preventing unauthorised access to details and keeping safe online

The Crime Survey for England and Wales (CSEW) asks questions on the security measures respondents take to prevent unauthorised access to account details and keep safe online. These questions are asked of all respondents, regardless of whether they have been a victim of fraud, computer misuse or any other offence. As such, it is not possible to say whether any security measures taken were in direct response to having been a victim of an offence or were actions respondents take regardless.

Preventing unauthorised access to bank, building society or credit card account details

The majority of adults reported taking security measures to prevent access to account details in the year ending March 2019 CSEW (Figure 12; Appendix table 14). The most common of these were:

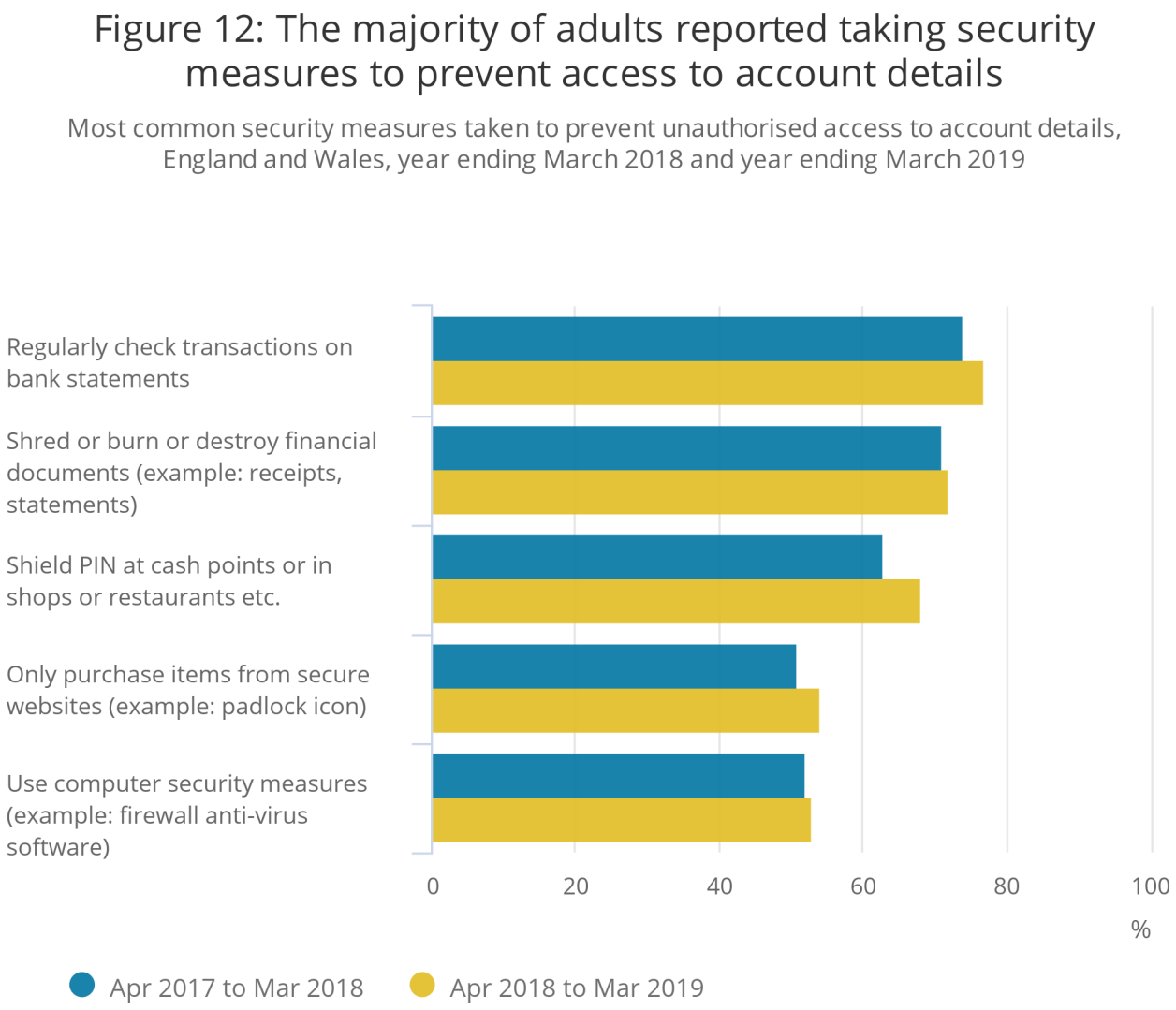
- regularly checking transactions on bank statements (77%)
- destroying financial documents (72%)
- shielding their PIN at cash points, in shops or in restaurants (68%)

A larger proportion of adults took each of these security measures than in the previous year.

Almost all (96%) adults took at least one of the security measures asked about in the year ending March 2019.

Figure 12: The majority of adults reported taking security measures to prevent access to account details

Most common security measures taken to prevent unauthorised access to account details, England and Wales, year ending March 2018 and year ending March 2019



Source: Office for National Statistics – Crime Survey for England and Wales

Notes:

1. Figures may not sum to 100 as more than one response is possible.

2. The question on measures taken to prevent unauthorised access to bank, building society or credit account details is only asked of one-quarter of the Crime Survey for England and Wales (CSEW) sample.

Keeping safe online

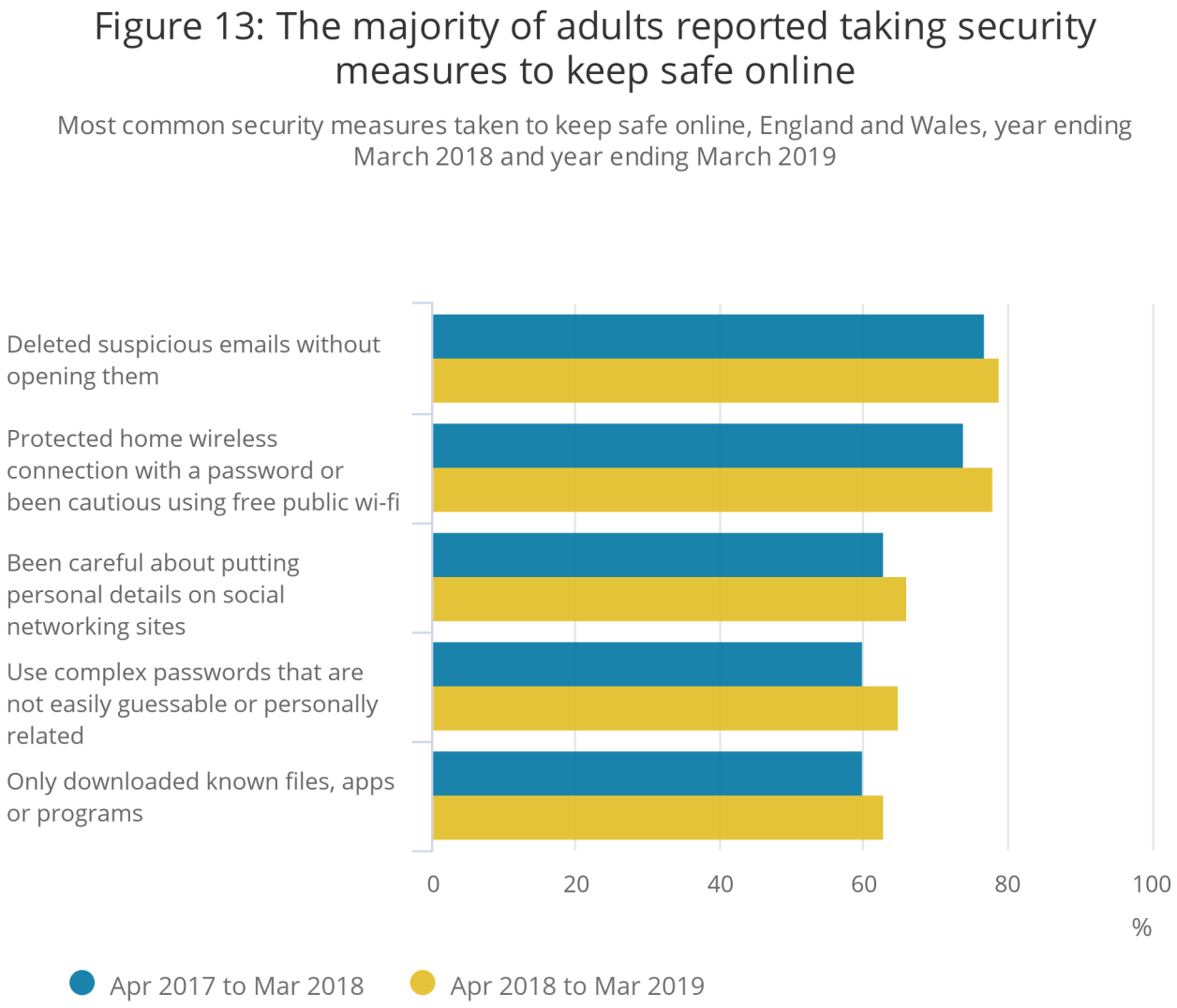
The majority of adults also reported taking security measures to keep safe online in the year ending March 2019 (Figure 13; Appendix table 15). The two most common of these were deleting suspicious emails without opening them (79%) and protecting their home wireless connection with a password or being cautious using free public Wi-Fi (78%).

A larger proportion of adults reported taking each of these security measures than in the previous year; this was also evident across almost all security measures asked about.

Almost all (94%) adults took at least one of the security measures asked about in the year ending March 2019.

Figure 13: The majority of adults reported taking security measures to keep safe online

Most common security measures taken to keep safe online, England and Wales, year ending March 2018 and year ending March 2019



Source: Office for National Statistics – Crime Survey for England and Wales

Notes:

1. Figures may not sum to 100 as more than one response is possible.

2. The questions on measures taken to keep safe online are only asked of one-quarter of the Crime Survey for England and Wales (CSEW) sample and of those, only those who had used the internet in the last year were asked.

12 . Fraud and computer misuse data

Crime in England and Wales: Appendix tables
Dataset | Released 23 January 2020
Trends in Crime Survey for England and Wales (CSEW) crime and police recorded crime, by offence type, including fraud and computer misuse.

Nature of fraud and computer misuse: Appendix tables
Dataset | Released 19 March 2020
Data from the CSEW and the National Fraud Intelligence Bureau (NFIB). Data are included on numbers of incidents and characteristics of victims.

Nature of crime: fraud and computer misuse
Dataset | Released 19 March 2020
Annual data from the CSEW. Data are included on the impact on the victim, contact with offenders, financial loss and experiences with computer viruses.

13 . Glossary

“All other fraud” (Crime Survey for England and Wales)

“All other fraud” encompasses “advance fee fraud”, which is when a payment is made to fraudsters who claim to be in a position of authority, to transfer money or for a promise of employment, wealth or gifts (including lottery scams and inheritance fraud), and “other fraud”, which covers fraud not otherwise categorised by the Crime Survey for England and Wales (CSEW) (including, but not limited to, investment fraud and charity fraud).

Bank and credit account fraud

Bank and credit account frauds involve falsely obtaining or using personal bank or payment card details in order to carry out fraudulent transactions. This can involve using a false identity, deceitful credit application, credit or debit cards, cloned cards, cheque books, or online accounts.

Consumer and retail fraud

Consumer and retail frauds occur when goods or services were paid for but failed to materialise, were misrepresented at point of sale, or were faulty or stolen. This includes bogus callers, ticketing fraud, phone scams and computer software service fraud.

Pull payment

Pull payments, while requiring authorisation from the payer (that is, the victim, in a fraudulent context), require the payee (that is, the offender, in a fraudulent context) to take some action in order to collect money from the payer. Examples of pull payments include setting up a direct debit or standing order.

Push payment

Push payments are initiated by the payer (that is, the victim, in a fraudulent context) to transfer money to the payee (that is, the offender, in a fraudulent context) such that the payee does not need to direct action themselves to receive the money. Examples of push payments include sending or paying cash and making a direct bank transfer.

14 . Quality and methodology

Crime Survey for England and Wales (CSEW)

The CSEW is a face-to-face victimisation survey. People resident in households in England and Wales are asked about their experiences of a selected range of offences in the 12 months prior to the interview.

New victimisation questions on fraud and computer misuse were incorporated into the CSEW from October 2015. Up until September 2017, the questions were asked of half the survey sample. Since October 2017, the questions have been asked of a full survey sample.

In March 2018, the new CSEW estimates on fraud and computer misuse were assessed by the Office for Statistics Regulation against the Code of Practice for Statistics and were awarded National Statistics status.

All differences reported in this article, based on the CSEW, are statistically significant at the 5% level unless otherwise stated.

For the nature of fraud analysis presented in Sections 6 to 9, advance fee fraud and other fraud have been combined to form the category “all other fraud” owing to the low numbers of victims of these offences.

National Fraud Intelligence Bureau (NFIB)

The NFIB is a government-funded initiative run by the City of London Police. They currently collate received reports of fraud from Action Fraud and two industry bodies: Cifas and UK Finance.

Action Fraud is the national fraud-reporting centre that records incidents of fraud directly from the public and organisations by phone or internet, in addition to incidents reported directly to individual police forces. Action Fraud works with the NFIB to provide support and fraud-prevention advice to individuals who are victims of fraud and to ensure a joined-up approach to policing and detecting fraud.

Cifas facilitates fraud data sharing between around 350 organisations from across the public and private sectors in the UK. It is a Specified Anti-Fraud Organisation (SAFO) under the Serious Crime Act 2007, and it operates as a not-for-profit membership association. Its coverage includes all of the major banks and around 90% of plastic card providers.

UK Finance is responsible for coordinating activities on fraud prevention in the UK payments industry, and it represents members from retail banks; credit, debit and charge card issuers; and card payment acquirers in the UK.

Strengths and limitations of the data sources

The CSEW is a large nationally representative sample survey that has used a consistent methodology over time. The survey covers crimes not reported to the police (or Action Fraud) and is not affected by changes in police recording practices; therefore, it is a reliable measure of long-term trends. However, for fraud and computer misuse, as full-year data have only been collected from the survey year ending March 2017 onwards, long-term trends are not currently available for these offences.

The CSEW does not cover crimes against businesses and those not resident in households (for example, residents of institutions and visitors).

Fraud data collated by the NFIB have wider offence coverage and population coverage (most notably, including offences committed against organisations) than the CSEW. In addition, the time lag between occurrence of crime and reporting results tends to be short, providing an indication of emerging trends.

However, data from Action Fraud exclude offences that are not reported to, or not recorded by, them. In particular, it is known that the proportion of offences committed against individual members of the public that are reported to Action Fraud is low.

Also, both sets of industry data from Cifas and UK Finance relate only to fraud that is identified and reported and only fraud affecting those organisations that are part of the respective membership networks. As such, neither dataset can provide a complete picture of fraud in the industry sectors they represent.

Overall, the CSEW provides the better indication of the volume of fraud and computer misuse offences experienced by the adult population, as it captures incidents that go unreported to the authorities. This can be seen, in particular, by the large difference in the volume of computer misuse offences between the CSEW and the offences referred to the NFIB by Action Fraud. However, the two sources have different coverage, which means it is difficult to make meaningful comparisons between them.

For further information on all these sources, see Sections 2 and 5.4 of the User guide to crime statistics for England and Wales.

15 . Related links

Crime in England and Wales: year ending September 2019
Bulletin | Released 23 January 2020
Trends in Crime Survey for England and Wales (CSEW) crime and police recorded crime, by offence type, including fraud and computer misuse.

Property crime tables
Dataset | Released 23 January 2020
Annual data from the CSEW, including demographic and offence type breakdowns and time series.

User guide to crime statistics for England and Wales
Methodology | Released 23 January 2020
Contains detailed information on the datasets used to compile crime statistics published by the Office for National Statistics (ONS).