Office for National Statistics

Article

Overview of fraud and computer misuse statistics for England and Wales

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:
Mark Bangs
crimestatistics@ons.gsi.gov.uk
+44 (0)1329 448689

Release date:
25 January 2018

Next release:
To be announced

Table of contents

1 . Introduction

In response to an ever-changing world, fraud has evolved more dramatically than other crimes over recent times with the rise of computers and the internet, and the introduction of “plastic payment”. Such technology has not only facilitated new methods of committing traditional crimes, but has also created opportunity for new types of crime altogether, such as computer misuse and cyber crime.

Focus around fraud from the government, the authorities and the media has been heightened, particularly over recent years in response to accumulating evidence that it has grown in volume. More emphasis has also been placed on accessing data on fraud and computer misuse from a variety of sources to help identify the true scale of the problem. Multiple sources may create a confusing picture, which can sometimes be difficult to clearly interpret. This overview seeks to guide readers through this complex field and explain what the fraud and computer misuse statistics currently tell us.

Administrative data sources can be partial in their coverage and subject to changes in recording practices or reporting arrangements. While questions on fraud and computer misuse, recently introduced into the Crime Survey for England and Wales (CSEW), provide fuller coverage of fraud against the household population, they do not generally include much of the fraud committed against the state, businesses and other organisations. While one data source may be indicating an increasing (or decreasing) trend, this may not be indicative of overall trends. Further discussion on the strengths and limitations of the main sources is available in the ‘Which source provides the better measure?’ section.

2 . How are fraud and computer misuse defined and measured?

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. The first established laws on fraud were set out in the First Statute of Westminster in 1275. While fraud is not a new offence, methods of committing fraud have evolved a great deal over recent times with the rise of the internet, providing opportunities for fraudsters to commit crime on an industrial scale.

However, the fundamental nature of the offence has remained unchanged and the majority of 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. This covers a broad range of fraudulent activity, including dating scams (where the intended victim is befriended by a fraudster online and tricked into sending them money for a variety of emotive reasons), lottery scams (where the potential victim is told they have won a non-existent lottery prize and needs to pay a fee to release the winnings) and inheritance fraud (offering the false promise of an inheritance to trick victims into paying money or sharing bank or credit card details). Most prevalent, however, are banking and payment card frauds, which usually involve falsely obtaining or using personal bank or payment card details in order to carry out fraudulent transactions.

Computer misuse crime covers any unauthorised access to computer material, as set out in the Computer Misuse Act 1990 (Annex 2 provides further information). This is not limited to desk or laptop computers and can include any device using operating software accessible online, for example, games consoles, smart phones and smart TVs. It includes offences such as the spread of viruses and other malicious software, hacking and distributed denial of service (DDoS) attacks (the flooding of internet servers to take down network infrastructure or websites). Many victims of the latter will tend to be public and private sector organisations and may not directly impact on the general public.

Such crimes are encompassed within the wider definition of cyber crime (also referred to as online, crime), which is an umbrella term used to describe two distinct, but closely-related criminal activities.

Cyber-dependent crimes

Cyber-dependent crimes are offences that can only be committed via a computer, computer network or other form of information and communications technology (ICT). These include not only offences mentioned previously, which fall under the Computer Misuse Act, but also some frauds that by their very definition only occur online, for example, online shopping and auction scams (where the victim buys supposedly legitimate goods through an internet site that are fake or fail to be provided).

Cyber-enabled crimes

Cyber-enabled crimes are traditional crimes that can be increased in their scale or reach by the use of ICT, but unlike cyber-dependent crimes, they can be committed without it, for example, ticket fraud (purchasing tickets in advance, which are never supplied or turn out not to be valid), as well as non-fraud crimes, such as offences involving online harassment or obscene publications.

There has been much increased focus on cyber threats following several recent high-profile cyber attacks and security breaches on national institutions, such as the WannaCry global ransomware attack in May 2017, which struck the National Health Service (NHS). However, cyber crime is not in itself a separate legal offence and does not form part of the notifiable offence list that is reported within official statistics on crime [1]. Instead such offences are recorded within the crime categories to which they relate based on the nature of the offence.

We do, however, publish some limited statistics provided by the Home Office on the number of offences for a range of crime types recorded by the police in England and Wales, which are flagged as having an online element, for example, harassment and stalking, blackmail and sexual offences. These are presented as Experimental Statistics and work is ongoing with forces to improve the quality of the data submitted in this collection[2]. Cyber crime is not discussed in any further detail in this article.

There are two principal sources of data currently used in the official statistics on fraud and computer misuse:

- incidents of fraud reported to the Crime Survey for England and Wales (CSEW), which is a household survey collecting information on crimes directly affecting the resident adult population over the previous 12 months
- incidents of fraud 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 [3] and Financial Fraud Action UK (FFA UK, a constituent part of UK Finance) [4], who report instances of fraud where their member organisations have been a victim

However, we also make use of other data to supplement these sources to provide the broader context for the official statistics, for example, CAMIS data collated by UK Finance. Further information on this data is available in the 'What are the long-term trends in fraud?' section.

Figures on fraud have long been included in historical police recorded crime data, but until recently fraud was not covered in the headline estimates from the CSEW. In order to address this gap, work has been completed to extend the main victimisation module in the CSEW with new questions on both fraud and computer misuse added to the survey from October 2015[5]. These questions cover a wide range of frauds involving both traditional and more modern methods (for example, those committed in person, by mail, over the phone and online), as well as offences falling under the Computer Misuse Act. First estimates on CSEW fraud and computer misuse were published in July 2016 and we now have two full years of comparable data to allow us to analyse trends for the first time as part of the quarterly bulletin Crime in England and Wales, year ending September 2017.

Previously these estimates of fraud and computer misuse have been classed as Experimental Statistics. We are satisfied with the work we have done surrounding the quality of the data and have now also added these to the total estimate of crime. At the same time we have asked the Office for Statistics Regulation to assess these new estimates for consideration as National Statistics. Until they have been assessed, these new estimates will be classified as official statistics.

Further discussion on the strengths and limitations of the main sources is available in the 'Which source provides the better measure?' section.

Notes for: How are fraud and computer misuse defined and measured?

1. The work of the National Cyber Security Centre and the National Cyber Crime Unit (part of the National Crime Agency) is focused primarily on collaborative detection, investigation and prevention of cyber crime at a national level.

2. These figures are available for the year ending March 2016 onwards and are presented as Experimental Statistics published alongside each quarterly publication (see Additional tables on fraud and cyber crime, year ending September 2017).

3. Cifas is the UK-wide fraud and crime prevention service, and facilitates fraud data sharing between public and private sector organisations in the UK. Cifas refers fraud offences to the NFIB via its National Fraud Database. For more information, please see Section 5.4 of the User Guide to Crime Statistics for England and Wales.

4. As of 1 July 2017, FFA UK is now integrated into UK Finance (a new trade association representing the finance and banking industry in the UK). As a constituent part of UK Finance, it coordinates fraud prevention activity and manages intelligence-sharing across the financial services industry. Information on fraud offences is submitted to the NFIB via a central Fraud Intelligence Sharing System (FISS) database. For more information, please see Section 5.4 of the User Guide to Crime Statistics for England and Wales.

5. Up to the end of September 2017, new questions on fraud and computer misuse were introduced to half of the CSEW sample to test for detrimental effects on the survey as a whole. From October 2017 onwards they are being asked of a full survey sample.

3 . What are the long-term trends in fraud?

Similar to other types of crime, trends in the number of offences recorded by the police date back to 1857 and indicate how fraud offences increased steadily through the 20th century [1].

While the historical police recorded data give a good indication of levels of fraud that were recorded by the police, changes in recording practices and reporting arrangements can make it difficult to interpret trends. For example, changes to the Home Office Counting Rules (HOCR) in 1998 led to a 61% increase in fraud and forgery offences recorded in the following year. Following this, trends were affected by the introduction of both the National Crime Recording Standards (NCRS) in 2002 and the Fraud Act 2006 [2], shown by a period of reductions in the number of police recorded fraud incidents. These decreases may be explained by findings from the 2006 Fraud Review [3], which pointed to, among other things, a lack of understanding by the police as to what constituted fraud, as well as a general lack of capacity or willingness by police forces to accept fraud reports.

As a result of the Fraud Review, the centralisation of fraud recording was introduced via the establishment of Action Fraud, who took responsibility for recording fraud offences previously recorded by individual police forces. The phased introduction of this central recording between April 2011 and March 2013 (Annex 1 provides further information) further complicates the interpretation of trends, as it is not possible to make meaningful year-on-year comparisons over this period.

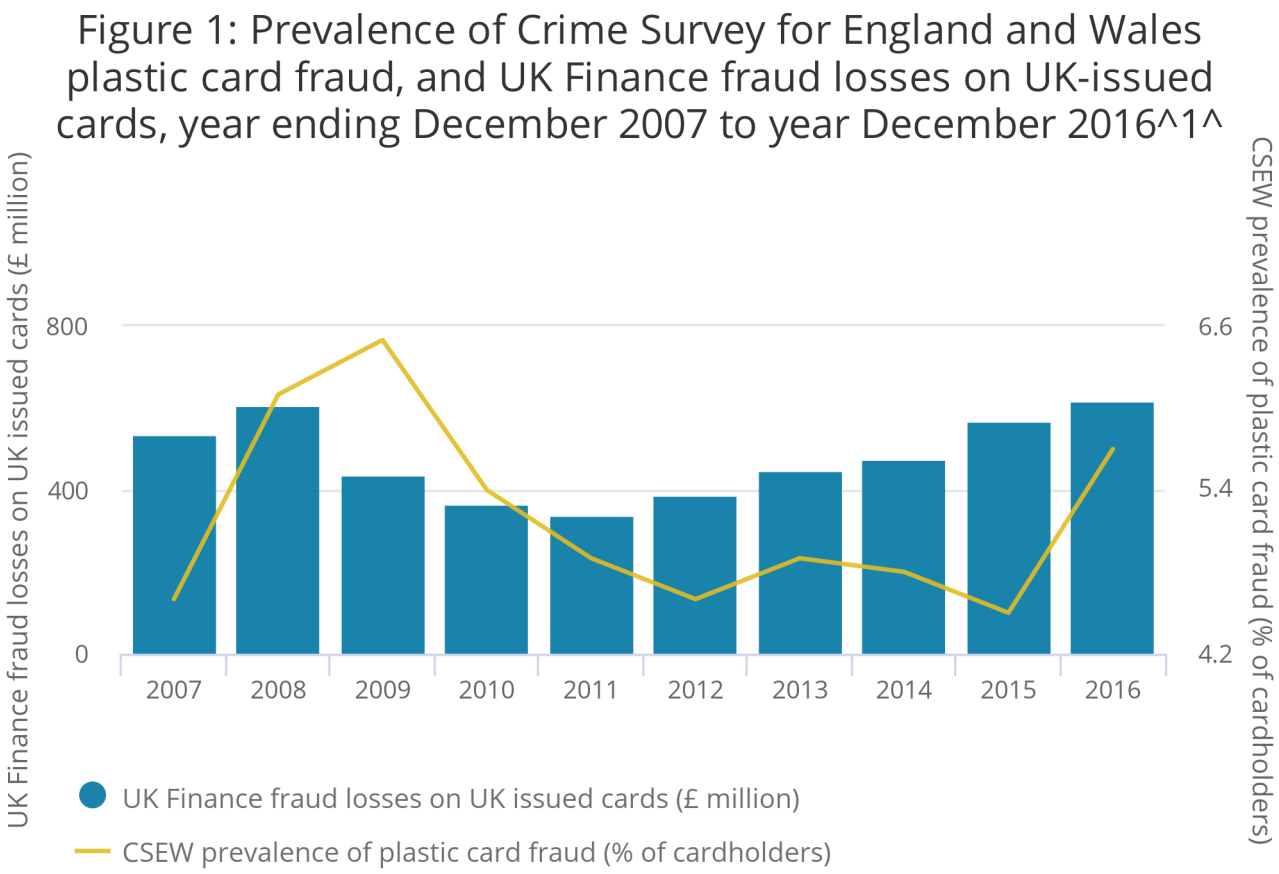
Since April 2014, when more comparable data have been available, some rises in fraud have been observed. This is indicative of an upward trend in fraud offences, although may also reflect improvements in the reporting and recording of fraud. For example, in July 2015 the company that was contracted to provide the Action Fraud call centre service went into administration, resulting in a period of lower than normal monthly volumes of recorded fraud offences. Volumes have subsequently recovered and while caution must be taken when considering discontinuities over time, which have been influenced by the changes in call centre operation, latest figures for the year ending September 2017 indicate that the volume of frauds recorded by Action Fraud is the highest it has ever been (272,980 offences).

Prior to the new questions on fraud and computer misuse being added to the Crime Survey for England and Wales (CSEW), one of the most reliable indications of trends in fraud offences experienced by the household population was sourced from a separate CSEW module of questions on plastic card fraud, first added to the survey in the year ending March 2006. These questions, which asked specifically about bank and credit card fraud rather than other types of banking fraud, did not collect enough detail to be added to the main crime estimates and have been reported on separately[4,5].

Figures from the module have shown steady year-on-year increases in the proportion of victims of plastic card fraud, with levels peaking around 2009, followed by declines coinciding with the introduction of EMV (EuroPay, MasterCard and Visa) chip card technology in a number of countries around the world. Figure 1 indicates that this closely matches the pattern of fraud losses on UK-issued cards reported by industry sources such as UK Finance. CSEW prevalence of plastic card fraud is presented here for the year ending December in order to be comparable to UK Finance data on fraud losses, which are available for calendar year only. Latest CSEW findings from the supplementary module for the year ending September 2017 showed that a similar level of plastic card owners were victims of card fraud compared with the previous year (5.7 and 5.3% respectively).

This supplementary module on plastic card fraud continued to be included in the survey while the new questions on fraud and computer misuse were bedded in. As of October 2017, the module was removed from the questionnaire and all future estimates relating to bank and credit card fraud will be calculated using data from the new questions.

Figure 1: Prevalence of Crime Survey for England and Wales plastic card fraud, and UK Finance fraud losses on UK-issued cards, year ending December 2007 to year December 2016 [1]



Source: Crime Survey for England and Wales, Office for National Statistics; UK Finance

Notes:

1. The CSEW data on this chart refer to crimes experienced in the 12 months before interview, based on interviews carried out in that year.

Following the inclusion of new questions on fraud and computer misuse in the main victimisation module of the CSEW in October 2015, the first full year-on-year comparisons of the last two years of data have been released as part of the quarterly bulletin Crime in England and Wales, year ending September 2017. Importantly, as this comparison is based on just two data points, caution must be taken in drawing inferences about trends at this early stage.

Estimates indicate 4.7 million incidents of fraud and computer misuse were experienced by adults aged 16 and over in England and Wales for the survey year ending September 2017, showing a 15% decrease from the previous survey year. Fraud, which accounted for over two-thirds of the estimated fraud and computer misuse total, fell by 10% from the previous year to 3.2 million offences. “Bank and credit account fraud”, which makes up the majority of total fraud offences, remained at a similar level to the previous survey year.

However, falls were seen in other types of fraud, for example, “consumer and retail fraud” [6] (down 20% to 0.7 million offences),“advance fee fraud” (down 53% to 56,000 offences) and “other fraud” (down 57% to 46,000 offences). Offences involving computer misuse showed a 24% decrease (down to 1.5 million offences), due mainly to a fall in “computer viruses” (down 26% to 1.0 million offences). Offences of “unauthorised access to personal information (including hacking)” did not show any significant change from the previous year. Trends will continue to be reported in our regular quarterly bulletins as more CSEW data become available.

Industry body data on fraud referred to the National Fraud Intelligence Bureau (NFIB) by Cifas and UK Finance (which appear in our headline figures, alongside those reported to Action Fraud) provide a useful additional indication of trends in banking and credit industry fraud but importantly, are known to exclude a significant volume of card and bank account fraud. In particular, UK Finance only refers crimes to the NFIB in cases where there is actionable intelligence to share with the police to aid fraud investigation and detection. For example, intelligence data exclude cases of fraud where card details have been obtained through unsolicited means and used to make fraudulent purchases online, over the phone or by mail order (known as “remote purchase fraud”) and cases of fraud using lost or stolen cards and ATM fraud.

However, an alternative source of data that UK Finance collates from its members is available via a system known as CAMIS and these data are able to capture card fraud not reported to the police for investigation [7]. As a result they provide a better picture of the scale of bank account and plastic card fraud in the UK, which helps us to bridge the gap between the broad coverage provided by the CSEW and the narrower focus of offences referred to the NFIB.

Available figures from CAMIS indicate a large rise in the number of fraud offences on UK-issued cards since March 2011 (the earliest year for which data are available) [8,9]. The introduction of chip card technology has forced fraudsters to change their methods of working and most of this increase is covered by offences falling into the categories of “remote purchase fraud” and “lost or stolen cards”, which account for a high proportion of plastic card fraud that is excluded from the NFIB figures.

Notes for: What are the long-term trends in fraud?

1. Historic trend data on police recorded fraud going back to 1898 can be found at Historical crime data on the GOV.UK website.

2. The Fraud Act 2006 came into force on 15 January 2007. The Act introduced additional fraud offences, but also changed the recording of cheque and plastic card fraud from a “per transaction” to a “per account” basis, for example, if an account is defrauded, one offence is recorded rather than one offence per fraudulent transaction.

3. The full Fraud Review can be found at the National Archives website.

4. While data from the plastic card questions provide a useful indication of whether an individual has been a victim of plastic card fraud, they do not provide information on the number of times this occurred or the scale of any loss that may have been experienced.

5. Although their definitions are closely aligned, the methodological approach taken in measuring CSEW plastic card fraud and the newer CSEW bank and credit account fraud are different and any comparison between the two measures should be interpreted with caution.

6. Non-investment fraud has been renamed as "Consumer and retail fraud" to reflect the corresponding name change to the Home Office Counting Rules from April 2017.

7. The CAMIS system contains cases where it has been judged that there is no evidential value and no hope of identifying the offender. CAMIS data includes those cases referred by UK Finance to the NFIB.

8. It is important to note that the number of cases relates to the number of accounts defrauded, rather than the number of victims.

9. UK Finance also publishes a longer time-series on fraud losses on UK-issued cards. For more information on this see the UK Finance Fraud The Facts 2017 publication.

4 . Which groups in society are most likely to be victims of fraud and computer misuse?

The Crime Survey for England and Wales (CSEW) analysis of fraud and computer misuse shows that this type of crime is more prevalent than many traditional crimes, with data for the year ending September 2017 showing individuals to be 10 times more likely to be a victim of fraud and computer misuse than a victim of theft from the person and 35 times more likely than robbery. They also found that there was typically less variation than seen in other types of crime in the rate of fraud victimisation across different groups in society (Tables E3 and E4, year ending March 2017). However, some personal and household characteristics were associated with being a victim of fraud and those with the higher risk of victimisation often differed from other crime types [1].

Age

Fraud victimisation was identified as being higher in the middle of the age distribution, where adults aged 35 to 44 were more likely to be a victim of fraud (7.4%) than 16 to 24 year olds (4.9%) or those aged 65 or over (65 to 74, 5.4%; 75 and over, 2.8%). This differs from violent crime and most property crime types where younger age groups were generally most likely to be victims. Similar to other types of crime, however, adults aged 75 and over were less likely than any other age group to be a victim of either fraud or computer misuse.

Household income

Unlike victims of violence, victimisation from both fraud and computer misuse was greater in higher income households of £50,000 or more (fraud, 8.8% and computer misuse, 4.4%) than lower income households of less than £10,000 (fraud, 5.3% and computer misuse, 2.5%).

Occupation

Individuals in managerial and professional occupations were more likely to be a victim of fraud (8.0%) than individuals in intermediate occupations[2] (6.1%), routine or manual occupations (4.6%), full-time students (4.6%) and those who have never worked or are in long-term unemployment (2.0%). This is in contrast to violence where students are at greatest risk of being victims.

Area of residence

In some cases the groups typically less likely to be victims of other crime types indicated higher prevalence of victimisation from fraud. For example, individuals living in the least deprived areas were shown to be more likely to be a victim of fraud (7.2%) than those living in the most deprived areas (5.3%). This was also shown to be true of victims of computer misuse (3.3% and 2%, respectively). This cannot be used as an indication of where the fraud took place, only where the victim resides.

Experimental statistics based on Action Fraud data broken down by force area are consistent with the CSEW findings in showing less variation than other crime types in rates across forces (where the victim lived) for the year ending September 2017, although rates for forces in southern England were slightly higher than those among forces in Wales or northern England (see Additional tables on fraud and cyber crime, year ending September 2017).

Notes for: Which groups in society are most likely to be victims of fraud and computer misuse?

1. Some of the characteristics may be closely associated with each other, so caution is needed in the interpretation of the effect of these different characteristics when viewed in isolation (for example, employment and household income are closely related).

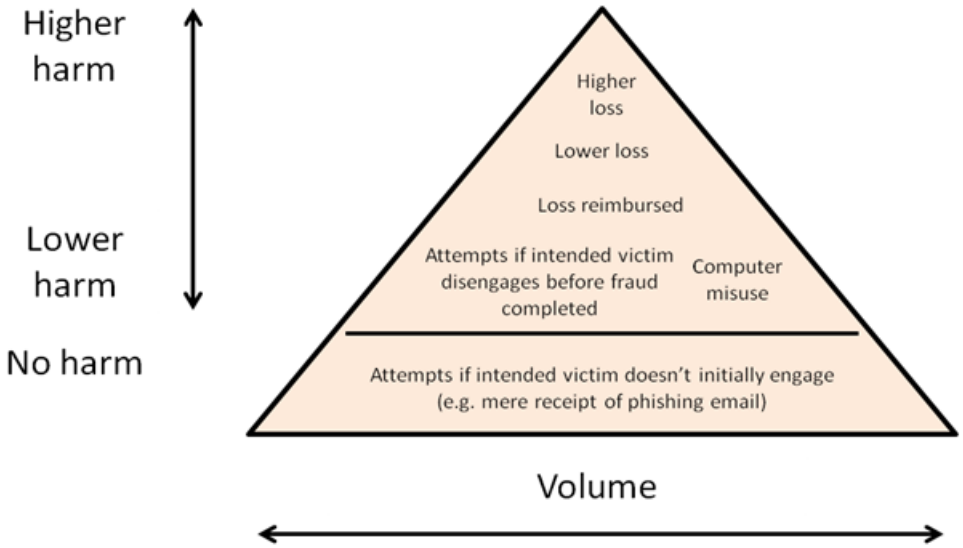
2. Intermediate occupations refer to positions in clerical, sales, service and intermediate technical occupations that do not involve general planning or supervisory powers.

5 . What is known about the nature and circumstances of fraud and computer misuse?

Analysis of the Crime Survey for England and Wales (CSEW) data on fraud and computer misuse highlights that most incidents of fraud generally involve little or no harm to their intended victims while fraud offences involving high levels of harm are very low in volume.

Figure 2 illustrates this relationship between the level of harm caused to victims and the volume of fraud offences.

Figure 2: Fraud harm pyramid



The high volume incidents are generally those involving no or little harm to those on the receiving end. Above that line there is a wide spectrum of harms, ranging from attempts to defraud where the intended victim is initially taken in but disengages before the fraud is complete, through to people who are defrauded out of money but who recover their losses, through to smaller numbers of individuals who are scammed out of significant sums of money, which they may not be able to claim back.

Analysis of the CSEW revealed that only 14% of incidents of fraud and computer misuse either come to the attention of the police or are reported by the victim to Action Fraud (see Table E7, year ending March 2017). Compared with the much higher estimates from the CSEW, offences reported to Action Fraud are thus likely to represent the more serious end of offending. For instance, victims are more likely to report cases where the scale of financial loss or emotional impact on them is greater. In contrast, the profile of cases covered by the CSEW will cover the full spectrum of harms, though those at the least harmful lower end will dominate the estimate.

This is reflected in the different distribution of cases in the two data series. Computer Misuse Act offences and bank and payment card fraud dominate CSEW estimates. For example, bank and credit industry fraud makes up around half of total fraud and computer misuse incidents in the CSEW data, compared with around 10% of total incidents from the Action Fraud data. In contrast, around two-fifths of Action Fraud offences are accounted for by consumer and retail frauds (such as fraudulent sales, bogus callers, ticketing fraud and computer software service fraud) and in particular frauds involving online shopping and auctions. This compares with around 15% of consumer and retail frauds identified by the CSEW.

Another sizable fraud category highlighted by Action Fraud figures is advance fee payment fraud (such as lottery scams, data scams and inheritance fraud), which accounts for just under one-fifth of total Action Fraud offences (compared with just 1% of CSEW fraud and computer misuse incidents).

Further analysis of the CSEW data on fraud and computer misuse has revealed additional information about the nature of such incidents:

- the large majority of victims of fraud and computer misuse had been a victim only once (81%), with the remaining 19% having experienced more than one offence (within the same 12-month crime reference period)
- by offence type, repeat victimisation was more common among victims of bank and credit account fraud (15%) than other types of fraud (for example, consumer and retail fraud, 5%) (Table E5, year ending March 2017)
- almost three-quarters of fraud incidents involved initial loss of money or goods to the victim (73%), independent of any reimbursement received[1]; this equates to an estimated 2.4 million offences, compared with 0.9 million incidents of fraud involving no loss (Table E1, year ending March 2017)
- where money was taken or stolen from victims of fraud, in just under two-thirds (63%) of incidents the victim lost less than £250 (Table E2, year ending March 2017)
- incidents of bank and credit account fraud were more likely to result in initial loss to the victim (78%, equivalent to 1.9 million incidents) than other types of fraud (for example, consumer and retail fraud, 62%; in the majority of these incidents, the victim received a full reimbursement (84%), typically from their financial services provider
- with regard to computer misuse, 23% of incidents involved loss of money or goods, all relating to computer viruses (410,000 incidents)[2]

New data have been released by UK Finance on Authorised Push Payment (APP) scams, which involve cases where victims are tricked into sending money directly from their account to an account which the fraudster controls. Unlike other frauds, victims of APP fraud are often deemed to have been at fault and are less likely to recover their losses.

The UK Finance data showed that of the £101 million lost to transfer scams in the first six months of 2017, only a quarter of the money was returned to the victim. This new data was produced in response to investigations by the Payment Systems Regulator (PSR) into a Super-complaint received from the consumer group Which? in 2016. Following the Super-complaint, the PSR, the Financial Conduct Authority (FCA) and the payments industry (represented by UK Finance) have developed an ongoing programme of work to reduce the harm to consumers from APP scams[3].

Notes for: What is known about the nature and circumstances of fraud and computer misuse?

1. 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, for example, bank charges, repair costs, replacement costs and so on.

2. Loss through computer viruses was associated solely with additional charges or repair and replacement costs incurred as a result of the virus, which are unlikely to be fully reimbursed.

3. For more information see the report and consultation published on 7 November 2017 explaining the work the PSR, the FCA and the payments industry have undertaken in the past year.

6 . Which source provides the better measure?

Each of the main sources of statistics on fraud has strengths and limitations and the preferred measure depends greatly on what the user requires.

In general terms, estimates from the Crime Survey for England and Wales (CSEW) provide the best indication of the volume of fraud offences directly experienced by individuals in England and Wales. The survey encompasses a broad range of fraud offences (including attempts as well as completed ones involving a loss), is able to capture incidents that are not reported to the authorities and is not affected by changes in recording practices or reporting rates.

The CSEW also provides the preferred measure of trends; while this is currently restricted to only two years of comparable data from the new questions in the survey (and the existing plastic card fraud module), as more data are gathered over time the CSEW will be able to provide robust data on wider trends in fraud against the adult population living in households.

Fraud estimates from the CSEW are substantially higher than those suggested by the recorded figures on fraud as the survey is able to capture a large volume of lower-harm cases that are less likely to have been reported to the authorities. While recorded data have broader coverage of parts of the population not captured by the CSEW (including frauds against business, or against people not resident in households), findings from the CSEW indicate that only a relatively small proportion of fraud and computer misuse incidents (including those where a loss was suffered) either come to the attention of the police or are reported to Action Fraud, with the most common reasons for not reporting including a lack of awareness of Action Fraud (66%), victims thinking the incident would be reported by another authority (10%) and victims thinking the incident was too trivial or not worth reporting (8%) (year ending September 2016[1]).

This low reporting rate means that recorded fraud data provide only a partial picture of the extent of fraud, however, they do provide a good measure of more serious fraud offences, where the financial loss to the victim is greater, as reporting rates for these offences tend to be higher.

Recorded crime data are known to exclude a significant volume of card and bank account fraud, although alternative sources of data such as those provided by the UK Finance CAMIS system help to provide a better picture of the volume of bank and credit account fraud identified by financial institutions in England and Wales. The trends in these data also help to provide an alternative to the CSEW and are likely to provide a better indication of short-term trends, although administrative sources can be subject to changes in practice and priorities. CAMIS data also only include confirmed cases (where a loss was suffered). Therefore figures exclude incidents of attempted fraud where the attempt has been stopped or prevented for whatever reason (for example, by bank detection systems) before a loss has occurred[2].

While CSEW fraud data at the national level (England and Wales) are of high quality, it is not possible to produce reliable estimates for subnational geographic areas due to the size of the survey sample. A low-level geography breakdown (police force area), based on where the victim resides, is now also available for Action Fraud data as Experimental Statistics from the year ending March 2016 onwards (see Additional tables on fraud and cyber crime, year ending September 2017).

Notes for: Which source provides the better measure?

1. This was produced in response to an ad hoc request on 8 February 2017.

2. UK Finance does collect data on prevented fraud, although this is not supplied to ONS due to the potential for double-counting. The prevented data are available in the UK Finance Fraud The Facts 2017 publication.

7 . What are the main differences between the main sources?

The coverage and information available from each of the main sources of fraud data differ.

The Crime Survey for England and Wales (CSEW) is a household survey and as such, information collected on fraud offences only relates to the resident adult population. Fraud against businesses is not covered by the CSEW. In addition, no information about fraud against those under 16 years of age is collected.

The CSEW can, however, identify fraud offences that have not come to the attention of Action Fraud or the National Fraud Intelligence Bureau (NFIB) for whatever reason (for example, the victim does not consider the incident serious enough or where there is not enough actionable intelligence for the offence to be referred to NFIB).

However, the CSEW is subject to potential response bias. As highlighted, the survey is dominated by a large volume of incidents of fraud involving little or no loss and while this reflects the general profile of fraud incidents, compared with some other crimes, it is possible that some victims of fraud, especially the elderly and vulnerable victims who may have been victims of high-loss frauds, may not have the confidence to allow an interviewer into their home to conduct an interview for fear that it is not genuine. In addition, some victims of fraud who have lost substantial amounts of money may not want to admit to the loss through either embarrassment or shame, or not wanting to look foolish falling for a scam.

The classification of fraud and cyber crime offences used for the CSEW, as with all crime types, mimics the Home Office Counting Rules (HOCR). The HOCR provide a national standard for the recording and counting of notifiable offences recorded by Action Fraud. Whilst the HOCR have been followed as closely as possible with regard to CSEW fraud, there are a few instances in which the CSEW offence coding rules and the HOCR differ.

Who are counted as victims?

The CSEW is a household survey and does not cover crimes against businesses. Therefore the household respondent will be recorded as the victim where they report experiencing a fraudulent offence, such as transactions appearing on their bank or credit card statement that were a result of some fraudulent activity by others.

In contrast, Action Fraud receives reports from both individuals and organisations and therefore either can be recorded as victims and represented in their figures. In the case of cheque, plastic card and bank account fraud, where, for example, an individual cardholder reports to Action Fraud that they have been the victim of fraudulent transactions on their bank account, the crime will only be recorded by Action Fraud if the individual has not been reimbursed by their financial institution.

Where the financial institution has reimbursed the individual for their losses, Action Fraud will deem the financial institution rather than the account holder as the victim. Only if the financial institution reports the incident to Action Fraud will a crime be recorded (although an intelligence report would still be filed). In terms of the same crime being reported in the CSEW, the respondent is recorded as the victim regardless of whether or not they received any reimbursement from their bank.

Number of victims

In terms of bank and credit account fraud, if a victim's bank account is used fraudulently to purchase goods more than once or from more than one shop, Action Fraud will record one incident per account defrauded. In contrast, as the CSEW is an individual survey, if multiple accounts are accessed in the same incident the CSEW records it as one incident against the victim rather than the number of accounts per incident.

Where the fraud occurred

Compared with traditional crimes, the location of a fraud can often be difficult to establish especially if the internet is involved. Unlike other crime types, both recorded crime and the CSEW collect information based on victim residence rather than where the fraud took place.

Action Fraud will only record a fraud as a crime where it is apparent that either the offender was resident or operating in England and Wales (regardless of where the victim lives), or that the victim whilst resident in England and Wales was defrauded either from within England and Wales or from abroad.

The CSEW on the other hand does not distinguish between where the incident happened, for example, it includes frauds against respondents who were abroad when the incident happened.

Specific intended victim (SIV)

For any fraud classification to apply, the HOCR require that the respondent must not only have been the victim of the offence, but must also be the "specific intended victim", whereby they must have responded to initial communication from a fraudster, or taken some action in a way that the perpetrator intended (for example, clicking on a link in an email, or ringing a given number).

In cases of phishing (emails that link to hoax websites in an attempt to gain access to valuable personal information such as usernames and passwords), it is not sufficient just to have received a phishing email for it to be recorded as a crime in the HOCR. Phishing is an enabler to commit fraud and no separate crime is recorded in relation to the phishing. This means that phishing in itself is not included in either the survey estimates or the recorded crime data.

With regard to computer viruses, Action Fraud only classes the victim as an SIV if the victim clicked on a link that resulted in their computer or internet-enabled device becoming infected. In contrast, the CSEW assumes that where the computer is infected with a virus, the victim must have acted in some way for the computer to have become infected, which automatically makes them an SIV.

The classification of fraud and cyber crime incidents for use in the published statistics consists of four major fraud categories and two computer misuse categories.

Fraud

Bank and credit account fraud

Comprises fraudulent access to bank, building society or credit card accounts or fraudulent use of plastic card details.

Advance fee fraud

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

Consumer and retail fraud (previously known as non-investment fraud)[1]

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

Other fraud

Comprises all other types of fraud against individuals not recorded elsewhere, for example, investment fraud or charity fraud.

Computer misuse

Unauthorised access to personal information (including hacking)

Comprises offences where the respondent's personal details have been accessed without their permission.

Computer virus

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

For purposes of comparability, the CSEW classification broadly aligns with the classification system employed by the National Fraud Intelligence Bureau (NFIB), although some NFIB categories do not apply to the general household population, for example, "fraud by abuse of position", whilst others such as "charity fraud" (where numbers were considered too small for measurement by the survey) have been subsumed into the "other fraud" category. As with the NFIB classification, the CSEW also includes offences covered by the Computer Misuse Act though these are not fraud offences.

Action Fraud captures reports from both public and businesses on fraud offences and assesses them against the requirements of HOCR. The data collected via Action Fraud covers a much broader range of frauds than the CSEW is able to do, capturing a number of specific fraud types falling under each of the main sub-categories mentioned previously.

Fraud offences referred to the NFIB by industry bodies cover only a subset of fraud types and in respect of UK Finance, offences relate only to "cheque, plastic card and online bank accounts (not PSP)".

Notes for: What are the main differences between the main sources?

1. Non-investment fraud was renamed as "Consumer and retail fraud" to reflect the corresponding name change to the Home Office Counting Rules from April 2017.

8 . Where can more information be found?

Crime Survey for England and Wales (CSEW)

Crime in England and Wales (quarterly publication):

- Appendix tables A1, A2, A3 and A8 include data on numbers of incidents for the latest 12-month period, incidence rates (per 1,000 adults), prevalence rates (proportion of adults that were victims) and numbers of victims for the available survey time series; estimates are provided for fraud and computer misuse, fraud, bank and credit account fraud, consumer and retail fraud, advance fee fraud, other fraud, computer misuse, computer virus and unauthorised access to personal information (including hacking)
- Figure 12 within the bulletin provides the proportion of CSEW plastic card users who had been a victim of plastic card fraud in the last year, back to year ending March 2006
- Additional tables on fraud and cyber crime (formerly Experimental tables) include data on numbers of incidents, incidence rates, number of victims and prevalence rates presented for each offence group split by loss, as well as proportion of cyber and non-cyber fraud; tables published alongside “Year ending March” releases only also include data on financial loss suffered by victims of fraud, personal and household characteristics associated with being a victim of fraud and computer misuse, repeat victimisation and reporting rates
- Quarterly table QT2 includes data on numbers of incidents in the previous two survey years, broken down by quarter of interview
- User guide tables UG2a, UG3a, UG4a and UG5a published alongside the bulletin provide confidence intervals around CSEW estimates of number of incidents, incidence rate and victimisation rates for fraud and computer misuse, also presented by respondent’s sex and age

Focus on: Property Crime (annual release up to year ending March 2016)

- Commentary in overview chapter on more detailed findings from the related financial year.

Police recorded crime

Crime in England and Wales (quarterly publication):

- Table F3 presents the volume of fraud offences on UK-issued cards reported by the UK Finance CAMIS system, back to the year ending March 2011

- Appendix tables A4, A5 and A7 include data on numbers of incidents since the year ending March 2003, following the introduction of the National Crime Recording Standard (NCRS) in April 2002; this is the earliest time period for which the data are directly comparable; data are also presented on numbers of fraud offences (by fraud type) referred to the NFIB by reporting body (Action Fraud, Cifas and UK Finance), for the latest 12-month period and percentage changes with the previous 12-month period, as well as the rate per 1,000 population (and percentage change) back to year ending March 2012

- Quarterly table QT1 includes data on numbers of fraud incidents by reporting body (police, Action Fraud, Cifas and UK Finance) in the previous two financial years, broken down by quarter of interview

- Police force area open data include a time series of numbers of fraud incidents back to the year ending March 2003 by police force area

- Community safety partnership / local authority open data include a time series of numbers of fraud incidents back to the year ending March 2003 by community safety partnership / local authority

- Additional tables on fraud and cyber crime (formerly Experimental tables) include fraud offences referred to NFIB by Action Fraud by police force area (based on victim residency), English regions and Wales, for the latest 12-month period and percentage changes with the previous 12-month period, as well as offences recorded by the police in England and Wales that were flagged as online crime for the latest 12-month period

Focus on: Property Crime (annual release up to year ending March 2016)

- Commentary in overview chapter on more detailed findings from the related financial year.

9 . What other sources are available?

There are further sources of data available on fraud that are beyond the scope of administrative sources already mentioned and although not covered by our statistical bulletins they provide additional useful information.

Internal Fraud Database (Cifas)

Cifas operate a second database, the Internal Fraud Database, which is a data-sharing scheme for organisations that are victims of fraud by their own employees. Data from here do not feed directly into Action Fraud or National Fraud Intelligence Bureau (NFIB) and so do not currently feature in our published statistics. Although some of these frauds may be reported to Action Fraud by the organisation themselves, many will be dealt with internally.

Cifas publish an annual report, Employee Fraudscape, which provides an overview of the insider frauds recorded by those organisations who share data through the Cifas Internal Fraud Database.

Fraud in the benefit system (Department for Work and Pensions)

The Department for Work and Pensions publish biannual National Statistics on fraud and error in the social security benefit system. In particular the summary (Fraud and Error in the Benefit System) includes a breakdown of estimates of fraud overpayments (when a claimant is paid more in benefit than they are entitled to) for Housing Benefit, Pension Credit, Employment and Support Allowance and Jobseeker's Allowance.

Fraud in Tax Credits (HM Revenue & Customs)

HM Revenue & Customs measure fraud across the child and working tax credits population, including estimated fraud favouring the claimant. These are published in annual reports (Child and Working Tax Credits error and fraud statistics) based on a stratified random sample of cases.

Commercial Victimisation Survey (Home Office)

The Commercial Victimisation Survey (CVS) is a telephone survey in which respondents from a representative sample of business premises in certain sectors in England and Wales are asked about crimes experienced at their premises in the 12 months prior to interview. In 2016, for example, three sectors were surveyed: wholesale and retail, transportation and storage and administration and support.

The CVS is run by the Home Office and data are published on the Home Office's Crime against businesses statistics web pages.

Data are available on the number of incidents and incidence rates of fraud, as well as the number and proportion of premises that experienced fraud in the previous year, by industry sector. The survey also collects information on online crime from respondents using computers at their premises.

Findings from the 2017 survey are scheduled for publication in May 2018.

Retail Crime Survey (British Retail Consortium)

The Retail Crime Survey (PDF, 8.47MB) includes estimated costs of fraud and cyber crime on the UK retail industry and is conducted annually by the British Retail Consortium, a leading trade association that represents all forms of retailers.

Security Breaches Surveys (HM Government)

The Information Security Breaches Survey is carried out by the government and PwC, and asks companies across the UK about cyber security incidents and emerging trends. The Cyber Security Breaches Survey 2017 focuses on business action on cyber security and the costs and impacts of cyber breaches and attacks.

Scotland

Crime statistics for Scotland are collected and published separately and include numbers and incidence rates for fraud recorded by the police. These do not include figures from Action Fraud, Cifas or UK Finance.

Recorded crime statistics for Scotland are not directly comparable with those in England and Wales. The recorded crime statistics for Scotland are collected on the basis of the Scottish Crime Recording Standard, introduced in 2004, which like its counterpart in England and Wales, aims to give consistency in crime recording. The main principles of the Scottish Crime Recording Standard are similar to the National Crime Recording Standard for England and Wales with regard to when a crime should be recorded.

However, there are differences between the respective counting rules. For example, the "Principal Crime Rule" in England and Wales states that if a sequence of crimes in an incident, or alternatively a complex crime, contains more than one crime type, then the most serious crime should be counted. For example, an incident where an intruder breaks into a home and assaults the sole occupant would be recorded as two crimes in Scotland, while in England and Wales it would be recorded as one crime.

Differences in legislation and common law have also to be taken into account when comparing the crime statistics for Scotland with England and Wales.

While the Scottish Crime and Justice Survey (SCJS) does follow a similar format to the CSEW, it does not currently include questions on fraud, although data on other crime types is broadly comparable despite differences in the crimes or offence classifications reflecting the differing legal systems.

Police recorded crime and SCJS data are published by the Scottish Government.

Northern Ireland

Crime statistics for Northern Ireland are collected and published separately and include fraud offences.

Police recorded crime data are published by the Police Service for Northern Ireland (PSNI). From 1 April 2015, Action Fraud took responsibility for the central recording of fraud offences previously recorded by PSNI, however, Action Fraud figures relating to victims residing in Northern Ireland are provided to PSNI on a monthly basis. Fraud statistics for Northern Ireland do not include figures relating to Cifas or UK Finance.

The legal system in Northern Ireland is based on that of England and Wales, and the PSNI has the same notifiable offence list for recorded crime as used in England and Wales. In addition, the PSNI has adopted the National Crime Recording Standard (NCRS) and Home Office Counting Rules for recorded crime that applies in England and Wales. Therefore there is broad comparability between the recorded crime statistics in Northern Ireland, and England and Wales.

The Northern Ireland Crime Survey (NICS) also closely mirrors the format and content of the CSEW, using a very similar methodology with continuous interviewing and a face-to-face interview with a nationally representative sample of adults (16 years and over), using a similar set of questions. Therefore, results from the two surveys are broadly comparable, although the NICS also does not currently include questions on fraud.

NICS data are published by the Department of Justice (Northern Ireland).

10 . Annex 1: Changes to arrangement for reporting and recording fraud and the coverage of police recorded fraud

Over recent years there have been some changes and updates to the presentation of crime statistics to reflect new operational arrangements in reporting and recording practice and these changes need to be considered when interpreting findings.

Firstly, fraud data presented in the police recorded crime series now show offences recorded by Action Fraud, a public-facing national reporting centre that records incidents of fraud reported to them directly from members of the public and organisations. Between years ending March 2003 and March 2012, the headline figures for England and Wales showed a steady decrease in fraud offences recorded by the police, with subsequent increases thereafter following the introduction of Action Fraud.

Its launch led a transfer over of responsibility for centrally recording fraud offences that were previously recorded by the police, using a phased approach over a two-year period, with Action Fraud taking over full responsibility from April 2013[1]. Data from Action Fraud are collated by the National Fraud Intelligence Bureau (NFIB), a government-funded initiative run by the City of London Police, who lead national policing on fraud.

The transfer to Action Fraud is thought to have led to more consistent recording of fraud and is designed to make it easier for victims to report, for example, by providing various reporting channels including a call centre and an online tool. While it is not possible to provide separate figures for individual victims, it is thought that members of the public make up the vast bulk of incidents reported to them.

In addition, coverage of fraud against corporate bodies and institutions has improved since the official statistics on police recorded crime were extended to include other fraud offences reported to the NFIB by two industry bodies, Cifas and UK Finance. Both bodies are membership organisations, covering all major banks and plastic card providers, and each independently collects data from its members on fraudulent activity which it passes on to the NFIB. These statistics provide a useful indication of the number of offences against financial institutions that are reported to the NFIB. However, in the case of offences involving bank account and plastic card fraud, such reports will tend to be focused on those with the best investigative leads and it is known they represent only a small fraction of the totality of such crime.

The majority of frauds reported to Cifas occur at the point of application for financial products or services, while UK Finance data focuses on fraudulent activity on existing accounts. Together they provide a good source of data relating to banking and credit industry fraud that have come to the attention of the police in England and Wales [2], reporting over 350,000 incidents between them to NFIB each year. Of these incidents, over two-thirds of offences relate to cheque, plastic card and online bank account fraud, with the remaining relating to referrals by Cifas for application fraud[3] and a small proportion of mortgage-related fraud[4].

Both sets of industry data from Cifas and UK Finance relate only to fraud affecting those organisations that are part of the respective membership networks (members of UK Finance may also be members of CIFAS). While membership of Cifas and UK Finance has remained fairly stable over the last few years, it is possible that coverage could change as new members join or previous members withdraw, which could impact on overall figures for fraud reported. Data for these industry bodies are, like Action Fraud, presented in the police recorded crime figures from the year ending March 2012 onwards. Prior to this period, fraud cases for these organisations were not sent to the NFIB.

For more information on these administrative data sources on fraud, please see the User Guide to Crime Statistics for England and Wales.

Notes for: Annex 1: Changes to arrangement for reporting and recording fraud and the coverage of police recorded fraud

1. Police forces continue to record forgery offences, offences which meet the “call for service” criteria and crimes passed to them by the NFIB for investigation, but no longer record for statistical purposes any offences amounting to fraud as of 31 March 2013.

2. The two industry bodies collate data for UK as a whole. Cifas data are broken down to England and Wales level based on the address provided by the fraudster. Data from UK Finance are adjusted to provide a breakdown to England and Wales-level geography. For more information see Section 5.4 of the User Guide to Crime Statistics for England and Wales.

3. With regard to Cifas referrals, application fraud relates to fraudsters applying for products or services excluding cheque, plastic cards and bank accounts.

4. Mortgage-related fraud is where an individual fraudulently obtains one or more mortgages for profit or to assist in money laundering.

11 . Annex 2: Legal definitions

Fraud

The offence of fraud is laid out in Chapter 35 of The Fraud Act 2006, which came into effect on 15 January 2007 and affects England and Wales, and Northern Ireland.

1 Fraud

(1) A person is guilty of fraud if he is in breach of any of the sections listed in subsection (2) (which provide for different ways of committing the offence).

(2) The sections are—
(a) section 2 (fraud by false representation),
(b) section 3 (fraud by failing to disclose information), and
(c) section 4 (fraud by abuse of position).

(3) A person who is guilty of fraud is liable—
(a) on summary conviction, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum (or to both);
(b) on conviction on indictment, to imprisonment for a term not exceeding 10 years or to a fine (or to both).

(4) Subsection (3)(a) applies in relation to Northern Ireland as if the reference to 12 months were a reference to 6 months.

2 Fraud by false representation

(1) A person is in breach of this section if he—
(a) dishonestly makes a false representation, and
(b) intends, by making the representation—
(i) to make a gain for himself or another, or
(ii) to cause loss to another or to expose another to a risk of loss.

(2) A representation is false if—
(a) it is untrue or misleading, and
(b) the person making it knows that it is, or might be, untrue or misleading.

(3) “Representation” means any representation as to fact or law, including a representation as to the state of mind of—
(a) the person making the representation, or
(b) any other person.

(4) A representation may be express or implied.

(5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

3 Fraud by failing to disclose information

A person is in breach of this section if he—
(a) dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and
(b) intends, by failing to disclose the information—
(i) to make a gain for himself or another, or
(ii) to cause loss to another or to expose another to a risk of loss.

4 Fraud by abuse of position

(1) A person is in breach of this section if he—
(a) occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person,
(b) dishonestly abuses that position, and
(c) intends, by means of the abuse of that position—
(i) to make a gain for himself or another, or
(ii) to cause loss to another or to expose another to a risk of loss.

(2) A person may be regarded as having abused his position even though his conduct consisted of an omission rather than an act.

Computer misuse

The basic definition of theft is laid out in section 1 of the Computer Misuse Act 1990.

(1) A person is guilty of an offence if—
(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;
(b) the access he intends to secure, or to enable to be secured, is unauthorised; and
(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—
(a) any particular program or data;
(b) a program or data of any particular kind; or
(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable—
(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.