UK Parliament
POST

POSTnote 720

By Natalie Low,
Clare Lally
29 April 2024

Social and psychological implications of fraud

Overview

- Fraud accounts for 4 in 10 offences against individuals. 6% of adults were a victim of fraud in 2023. There are many types of fraud, such as purchase or romance frauds. Fraud changes quickly and much is cyber-related.
- The UK Government's 2023 Fraud Strategy includes aims to improve victim support, reimburse more victims and improve communications. It also seeks to prevent more frauds from taking place. This will involve actions by government, law enforcement, the private sector, and individuals.
- The stereotype of elderly fraud victims is inaccurate compared to observed fraud risks. Psychological and social factors may affect risk, for example, individual personalities, circumstances, or market-related vulnerabilities, such as demand for rental accommodation.
- In addition to financial loss, fraud can cause emotional, psychological and health impacts, and can harm people's relationships. Impacts may vary for individual victims, and by different fraud characteristics.
- Victims are most likely to report fraud to their bank or account provider, rather than the national reporting service Action Fraud or police.
- The published evidence base for fraud against individuals is limited. However, academics and practitioners suggest several areas to consider in implementing effective fraud prevention, including education, and victim care.

Background

The UK Government stated that fraud is a "significant threat to the people, prosperity and security of the UK".[1] According to the Crime Survey of England and Wales (CSEW),[a] for the year ending September 2023, fraud was the most common offence against individuals, accounting for 38%[b] of offences (see Patterns and trends in fraud against individuals).[4]

Government, law enforcement, private sector and third sector bodies are involved in the response to fraud against individuals, which includes prevention (see Preventing Fraud), education and victim support (Table 1).

Following rises in fraud during the Covid-19 pandemic,[4] since 2023, there has been a renewed government focus on addressing fraud and its impacts (Figure 1).

The cross-sector Home Office-led Fraud Strategy aims to reduce fraud by 10% from 2019 levels by December 2024.[c] [1,5] It includes specific aims to:

- improve victim support (see Reporting fraud and victim care)
- reimburse more victims (see Reimbursement)
- improve communications (see Fraud education and awareness)

Other policy developments include the Online Safety Act 2023[6–8] and the Online Fraud Charter (Figure 1).[8] Parliamentary scrutiny of progress in addressing fraud and its impacts includes, most recently, a 2023 Home Affairs Committee inquiry.

The published evidence base for fraud against individuals is limited.[9–23] The Fraud Strategy included a commitment for the Home Office to initiate an evaluation strategy to help build the evidence base on fraud and effective interventions to address it.[1]

While this POSTnote focuses on fraud against individuals, fraud also occurs against public sector, commercial and charitable bodies.[d] [26,27] The note focuses on England and Wales. Fraud is treated differently in law across the four nations of the UK, while policing and criminal justice matters are devolved to Scotland and Northern Ireland.[1]

---

[a] The Crime Survey for England and Wales (CSEW) is a face-to-face survey, covering household residents in England and Wales. Questions on fraud victimisation were first added in 2015.[2] Unless otherwise stated, 2023 CSEW estimates quoted in this POSTnote are for the year ending September 2023. These are based on 31,166 interviews, conducted between October 2022 and September 2023.[3]

[b] 38% is the number of fraud incidents as a percentage of "All CSEW crime including fraud and computer misuse" incidents.

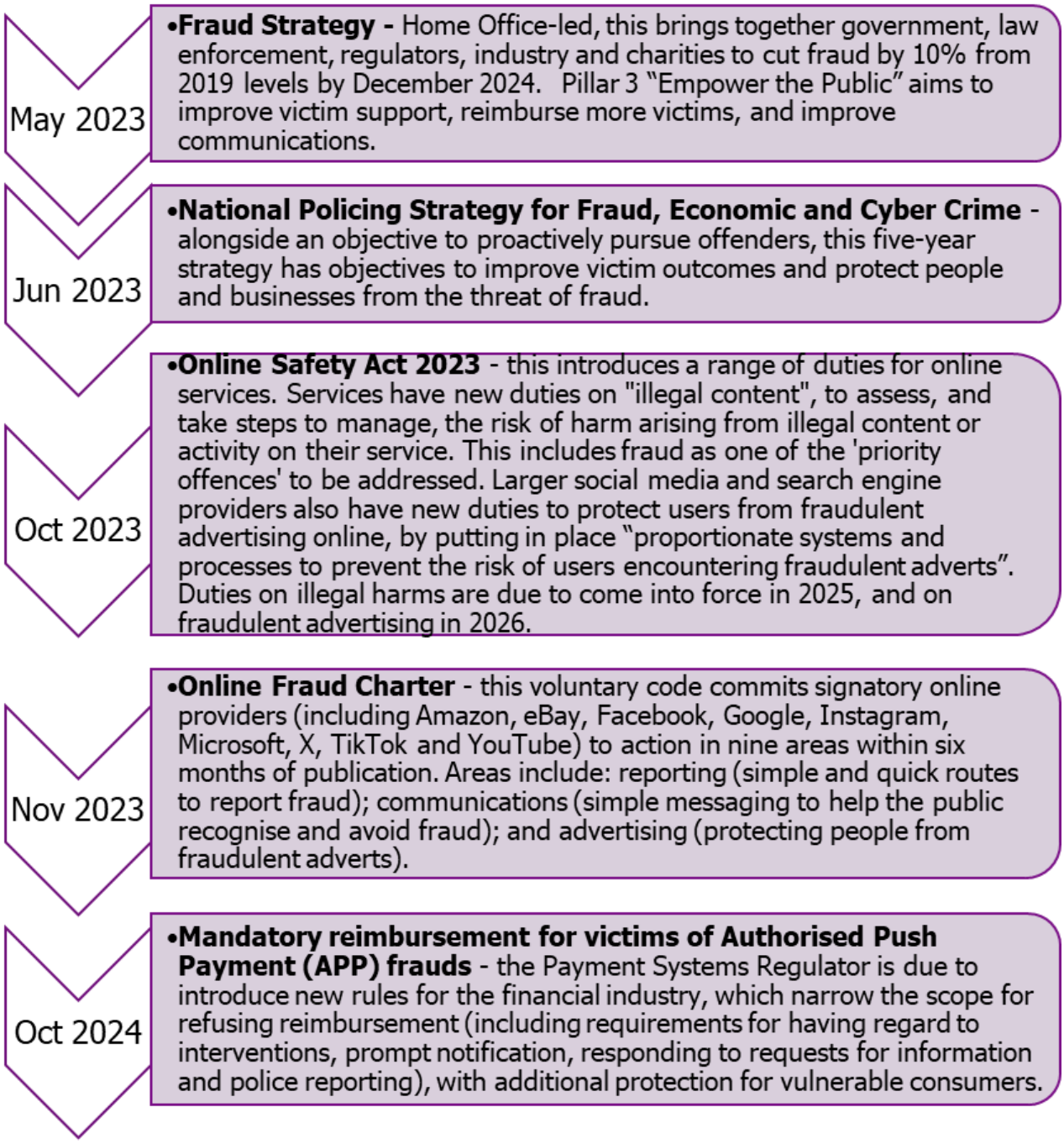
[c] Government announcements specify December 2024, although the strategy itself refers to a 10% cut in fraud incidents "from 2019 pre-Covid levels by the end of this Parliament".

[d] Around 10% of fraud reports to the national reporting service Action Fraud relate to businesses.[24,25] This note does not cover computer misuse offences, like hacking or viruses affecting computers or phones.[2]

Table 1 Sector roles and responsibilities for fraud against individuals in England and Wales

Sector	Main bodies, roles and responsibilities
Government	The **Home Office** oversees the overall response to fraud against individuals and businesses (primarily for England and Wales), including working with law enforcement and managing victim support.[1,28]
	The **Ministry of Justice** sets policy on criminal justice for fraud, works with courts, and manages the overall victim strategy.[28,29]
	Other departments include the **Department for Culture, Media and Sport (DCMS)**, for tech, online and telecoms sector issues and **HM Treasury**, for economic crime, and financial and banking regulation issues.[28]
Private sector	**Banks, building societies and payment service providers** carry out fraud prevention and education, via mandatory/regulated or voluntary activities, and reimburse fraud victims.[1,29]
	Telephone, online and other communication providers also undertake fraud prevention and awareness activities.[1,29–32]
Law enforcement and crime reporting	**City of London Police** is the national lead force for fraud in England and Wales. It coordinates fraud reporting, victim support and investigation, through oversight of: • **Action Fraud**, the national reporting service for fraud, which is due to be replaced in 2024 • the **National Economic Crime Victim Care Unit (NECVCU)**, which supports fraud (and cybercrime) victims • the **National Fraud Intelligence Bureau (NFIB),** which collates and analyses intelligence relating to fraud and cybercrime[28,29,33,34]
	Local police forces and the ten **Regional Organised Crime Units** investigate cases of fraud referred to them by the NFIB, support victims, and provide wider prevention activity.[1,28,35–37]
	As part of its remit for serious and organised crime, the **National Crime Agency (NCA)** is the operational system lead for the law enforcement response to fraud.[38]
Victim care and support	Specialist agencies such as **NECVCU** and **Victim Support** provide advice and support to victims alongside local bodies and services (see Victim care).[16,33,39–41]
Consumer support	Various bodies provide consumer advice and education, including **National Trading Standards, Age UK, Which?** and **Citizen's Advice Bureau**.[42–45]
Regulators	Regulators generally do not have direct powers to prevent or reduce fraud, but support or monitor activities in different sectors. Relevant regulators include **Ofcom** (telecommunications, postal and broadcast industries, and online providers), the **Financial Conduct Authority** (**FCA**, financial service industry) and the **Payment Systems Regulator (PSR)**, as well as the **Lending Standards Board (LSB)**, a self-regulatory body for the banking and lending industry.[28–30,46–49]

Figure 1 Policy developments in fraud against individuals from 2023



Source: collated from published information by gov.uk,[1,7,8] City of London Police,[37] Ofcom,[6,50] Which?[51] and Payment Systems Regulator.[52]

Types of fraud

There are many different types of fraud against individuals (Table 2). The CSEW found that 59% of frauds were bank and credit account frauds, 26% were purchase frauds and 11% advance fee frauds.[4]

Table 2 Types and examples of fraud against individuals.

The Fraud Act 2006 defines a general offence of fraud, which can occur through false representation, failing to disclose information, or abuse of position.[53] The list of examples below is not exhaustive.

Unauthorised fraud, where victims do not directly make or authorise any payment.	
Bank and credit account fraud	This usually involves fraudsters falsely obtaining or using personal bank or payment card details to carry out fraudulent transactions, including forms of identity fraud. It can involve using a false identity, deceitful credit applications, lost or stolen credit or debit cards, and cloned cards, cheque books, or online accounts.
Authorised push payment (APP) frauds where fraudsters trick victims into sending money directly from their account to an account that the fraudster controls.	
Consumer, retail or purchase fraud	Victims pay in advance for goods or services that are never received; fail to materialise; are misrepresented; or are faulty or stolen. This includes bogus callers and tradesmen, online shopping and auctions, ticketing fraud and phone fraud.
Advance fee fraud	Fraudsters convince victims to pay money upfront as a fee, promise or deposit for goods and services, employment, wealth or other benefits. This includes lottery, holiday, fraud recovery, inheritance, and rental frauds.
Impersonation fraud	Fraudsters contact victims, pretending to represent a reputable organisation, such as the police, a bank, utility company, or government department, and convince them to pay money to the fraudsters' account. Common frauds include claims that the victim must settle a fine, pay overdue tax or return an erroneous refund, or requests for remote access to the victim's computer to help 'fix' a problem. A variation of this fraud involves fraudsters pretending to be family or friends in need of help and money.
Investment fraud	Fraudsters convince victims to move their money to a fictitious fund or to pay for a fake investment. This includes boiler room frauds, pyramid or Ponzi schemes, and fake investment in items such as gold, property, carbon credits, cryptocurrencies, land banks and wine.
Pension fraud	Fraudsters persuade victims to invest pension savings or pension pots in fraudulent accounts.
Romance fraud	Victims are persuaded to make a payment to a person they have met, often online, and with whom they believe they are in a relationship.
Invoice fraud	Victims try to make a payment to a legitimate payee but the fraudster intervenes to convince them to redirect the payment to another account.

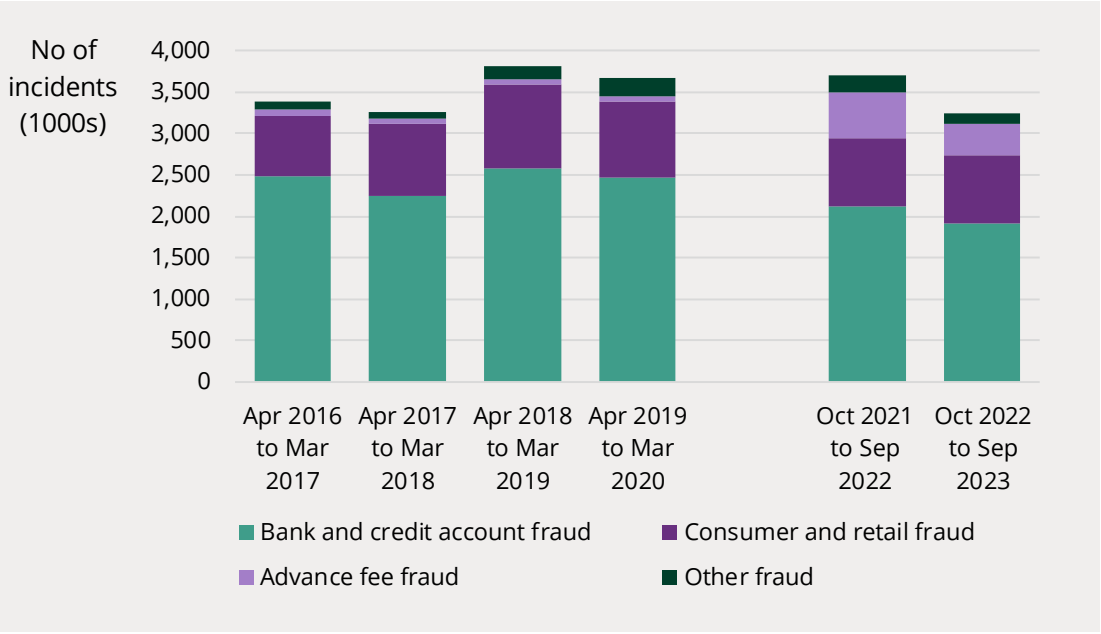
Source: adapted from information published by Office for National Statistics,[54] UK Finance,[55] Which?[56] and the Home Office.[27]

Government and stakeholders have highlighted particular concerns about 'authorised push payment' (APP) frauds, where fraudsters trick victims into making payments or sharing information like account details (Table 2).[1,51,55,57] These often involve 'social engineering', where fraudsters create a direct relationship with victims to manipulate them (see Psychological and social impacts of fraud against individuals).

Patterns and trends in fraud against individuals

In 2023, the CSEW estimated that there were 3.2 million fraud offences (Figure 2), equivalent to 6% of adults being a victim of fraud.[3,4] Other surveys suggest similar or higher levels of victimisation.[16,26,54,58–61] In CSEW findings for the year ending March 2023, 11% of fraud victims were repeat victims.[54]

Figure 2 Trends in fraud against adults aged 16 and over, England and Wales, 2016 to 2023



Source: Crime Survey of England and Wales, Year ending September 2023 of dataset.[4] Because of the Covid-19 pandemic, the CSEW did not run for the years ending March 2021 and March 2022.

Surveys indicate that most people encounter potential frauds, particularly online (whether or not they engage with them).[16,58–63] In a survey for a 2020 Communications Consumer Panel report, 79% of people thought they had been contacted in the past 2 years by somebody trying to defraud them; of those contacted, 11% reported being defrauded.[a 61]

[a] The Communications Consumer Panel survey was based on a nationally representative sample of 4,492 adults (4,038 online, 303 people aged 55-74 via telephone, and 151 people aged 75+ face-to-face). It asked about fraud experience over the previous two years.

Fraudsters use various channels to approach potential victims.[16,58,64] The Communications Consumer Panel survey estimated that 27% of frauds were online, 26% via email, 16% by phone, 13% by text, around 10% by post, and 7% by someone coming to the door.[61]

Cyber is a significant element in fraud against individuals.[65] For the year ending March 2023, the CSEW found that 42% of frauds against individuals were cyber-related,[a] with a higher proportion for purchase frauds (86%).[66]

Fraud is dynamic: fraudsters quickly adapt to opportunities arising from changes in communications, technology and financial services, or public events.[b] [11,32,70–73]

Artificial intelligence (AI) could make it easier for fraudsters to commit more convincing frauds at scale (PN 708). Stakeholders highlight that AI can be used to generate high quality pictures and videos (deep fakes), convincing messages (without grammar or spelling mistakes), credible social media profiles or impersonations, and customised content to target victims or engage them in online conversations.[38,70,74–77]

APP frauds, for example investment fraud,[78] are increasing (Table 2).[55,79] Based on UK Finance figures for 2022 (covering frauds against individuals and organisations),[c] APP frauds accounted for 7% of reported frauds, but 40% of monetary losses.[d] [55]

Fraudsters may use sophisticated techniques in APP fraud to engage and manipulate victims (Box 1).

Box 1: Techniques used in APP fraud

- **Building initial trust and rapport**, grooming victims through customised or frequent messages.[59,70,72,78,81–84] These may exploit pre-existing biases, like individuals' desire to please or obey perceived figures of authority.[17]
- **Manufacturing urgent demands**, to put victims in a 'hot state', when they have less time and space to think through transactions.[17,59,72,82]
- **Once trust is established**, coaching people past warnings and interventions, providing reassurance, isolating them from trusted sources, or using coercive control to manipulate them.[16,17,40,59,78,84] Once a relationship is established, this can make it harder for victims to realise they are being defrauded.[17,83,84]

[a] In the CSEW, 'cyber-related' represented any cases where the internet or any type of online activity was related to any aspect of the offence.

[b] For example, new types of pension fraud linked to people being able to take all or some of their pension pots as a lump sum,[67] frauds linked to the Covid-19 vaccination,[68] or fraudulent clearance sale sites set up after Wilkos entered administration.[69]

[c] UK Finance is a membership body representing the banking and finance industry.[80] The UK Finance figures relate to fraud that is identified and reported by its membership organisations, and includes frauds other than against individuals (for example, against businesses).[2]

[d] In 2022, there were 207,372 APP frauds reported to UK Finance (out of a total of 2,988,705). Overall fraud losses accounted for £1.2 billion in 2022, of which £485.2 million were related to APP frauds.

Who is at higher risk of fraud?

Studies show higher risks of fraud for some socio-demographic groups, although there is generally less variation in fraud risks compared to other crime types.[26,27,85]

Compared to an overall estimate of 6.3% of adults experiencing fraud in the year ending March 2023, the CSEW found slightly higher fraud risks for:[54]

- women aged 25-34 or 35-44 (7.6%)
- people in the highest income bracket (8.3%) or education level (7.6%),[a] and in managerial professions (7.6%)
- potentially vulnerable groups, including single parents (8.5%) and LGBT individuals (8.0-9.4%)

Some stakeholders emphasise that the stereotype of elderly, vulnerable fraud victims is inaccurate and unhelpful, compared to observed risks of fraud.[12,26,27,86]

Stakeholders also note that stereotypes of victims as stupid, greedy, reckless or naïve place too much accountability on the victim, and do not focus enough on the fraudsters (see Box 1).[12–14,16,18,41,87]

Psychological and social factors

Although the impact is less often quantified, academic and other studies highlight psychological and social factors that may affect people's risk of becoming a victim of fraud, including:

- **Individuals' disposition,**[b] such as having a greater respect for authority or being more trusting. [59,61,88] One review found that disposition-related factors predicted susceptibility to online fraud better than those related to competency with the internet or how fraudsters approached them.[82]
- **Circumstances and situations**[c] increasing people's vulnerability, for example, a recent bereavement, illness or stress,[16,17,61,88] or situations where people are socially isolated or have a cognitive impairment.[59,61,88]
- **Market-related** vulnerability: frauds making unique offers that exploit for example, rises in the cost of living or the demand for rental accommodation.[16,61,90]
- Individuals **under-estimating their personal risk** of fraud.[61,91] For example, in a poll of 4,596 adults for Lloyds Bank, 87% of respondents felt confident that

[a] Highest income bracket comprised people with a total household income of £52,000 or more; highest education level comprised people whose highest qualification was a degree or diploma.

[b] Dispositional factors include personality, demographics, and cognitive and decision-making ability.[82]

[c] Situational factors contrast with individual characteristics, and relate to external, sometimes temporary, factors, that may affect people's risk of victimisation.[16,89]

they could recognise the signs of fraud, but 10% were not aware of the most common types of fraud.[92]

- Particularly for online fraud, **exposure** to different communication channels,[58,62,88] as well as levels of **familiarity** with the internet.[61,82]

Psychological and social impacts of fraud against individuals

Scale and types of impact

Studies emphasise that fraud is not 'victimless', and its impact on victims extends beyond monetary loss.[16,26,27,30,93–95]

In addition to financial impacts, there is a broad consensus that fraud can impact on victims (Figure 3) in terms of:

- **emotional and psychological effects**, such as shame, anger, depression, loss of confidence, anxiety, fear and trauma[16,26,27,30,58,59,61,78,88,93,94,96]
- impacts on **mental and physical health**[16,26,27,58,59,93,94,96–98]
- harm to **relationships** and leading to loneliness and isolation[26,27,30,61,78,88,93,94,96,98]
- **changing behaviour,** including in potentially negative ways[26,27,30,58,59,61,93,98]

Surveys suggest variation in how much fraud victims are affected by the crime.[58,59,88,96] For example:

- In polling of 500 fraud victims for the Social Market Foundation covering the period 2020-2023, 35% reported negative impacts on their self-confidence, 25% on their mental health, and 9% each on their relationships and physical health. Around 30% reported no wider psychological or social impacts.[96]
- An analysis of 2017-19 CSEW data categorised 55% of fraud victims into "low vulnerability" groups, reporting relatively little harm from the fraud.[a] By contrast, 22% were in "high vulnerability groups", including greater emotional and relationship impacts, alongside higher financial losses.[88]

[a] Vulnerability can be defined in different ways. In this data, it was defined as combining the level of risk and harm to victims. The analysis identified nine "clusters", differentiated according to individuals' vulnerability to fraud (for example, whether they were a repeat victim), risk factors relating to the incident and victim, and harm caused.

Figure 3 Range of impacts from fraud

Source: Adapted from Blakeborough et al (2018)[27], and published material from a range of other sources[16,26,30,58,59,61,78,93,94,96]

Studies note long-term effects in terms of changes in behaviour[27,58,61] and mental health impacts for some victims.[59] For example, Home Office research on victims who reported their fraud to Action Fraud found that, 9 to 22 months later, 41% of those reporting self-harm still felt the effects, as did 39% of those reporting depression, 22% fear and 18% anxiety.[a] [98]

Factors that may affect impact

Financial loss

There is a large variation in the amount of money fraud victims lose:[27,93]

- A survey for a 2023 Crest Advisory report suggested that 42% of victims of online fraud were financially impacted, with around 25% losing less than £500, 8% between £500 and £1,000, and 3% over £10,000.[b] [26]
- The survey for the Communications Consumer Panel found that telephone and postal frauds tended to involve greater losses than online ones (median of £301 compared to £76).[61]
- There can be severe knock-on effects from any financial loss, including debt or bankruptcy.[16,61,96]

Some victims get all or some of their money back.[27,55,60,61] The 2023 CSEW found that 71% of fraud victims were refunded in full, higher for bank and credit account fraud (84%) and lower for consumer and retail fraud (42%).[99]

Many stakeholders noted the link between financial and psychological impacts.[10,13,19,88] Research for Ofcom on online fraud suggests that the key driver to emotional distress was the amount of money lost, which could be reduced if money was subsequently refunded.[59]

However, it is hard to predict the level of harm from the amount of money lost.[88,100,101] Research highlights how the impact of financial loss is relative: for some victims, small losses might be devastating, while others might lose substantial sums and be less affected.[93,98,102] Studies emphasise that victims can still experience emotional and psychological harm, even if no or little money is lost, or funds are reimbursed.[27,59,93]

[a] Based on a forthcoming research publication from the Home Office. The project included two telephone surveys with a combined sample of 2,450 fraud and cybercrime victims (of which 1,785 were fraud victims), representative of victims who reported their crime to Action Fraud in England and Wales between July 2017 and May 2018. It also included 16 in-depth interviews with victims receiving NECVCU support (including 15 fraud victims).

[b] The online panel survey for Crest Advisory (a consultancy specialising in crime and justice issues) was based on a national representative sample of 3,313 adults in England and Wales.

Type of fraud

Stakeholders noted that frauds involving a high level of 'social engineering' could be particularly harmful.[10,13,16,18,19,38,41,87,103]

For example, in romance fraud, fraudsters use forms of coercive control and grooming to gain victims' trust, manipulate and isolate them, approaching victims via dating apps or online.[78,83,84,104] Victims of romance fraud can experience a 'double hit', where they lose their money and their relationship. Romance fraud victims also often experience a lack of understanding from family, friends and others.[78]

The Home Office survey of victims reporting to Action Fraud found differences in reported emotional and health impacts for different types of fraud. For example, victims of bank and credit account fraud were most likely to report panic and anxiety-related impacts.[98]

Victims' characteristics

The relationship between victim characteristics and impact may not be straightforward. For example, in the analysis of 2017-19 CSEW fraud victims, groups identified as experiencing the highest harm included both older and younger people, and other contrasting socio-economic and demographic characteristics.[a] [88]

Some research suggests differences in impacts for different socio-economic groups.[61,98] In the Social Market Foundation survey of online fraud victims, victims were more likely to report impacts on their self-confidence if they earned £20,000 or below (46%, compared to 35% for all victims), were aged 65 and over (43%) or were female (41%).[96]

Fear of fraud

People may fear fraud even if they have not been a victim. Fraud is unusual in that it is both common (see Patterns and trends in fraud) and creates high levels of concern.[62,92,105]

In the survey for Crest Advisory, 55% rated online fraud as one of their biggest worries (higher than knife crime or burglary).[26] Anxiety may particularly affect vulnerable groups such as the elderly or those living alone, for example, if this stops them from using potentially beneficial communication channels.[106,107]

[a] These groups included: "severely harmed victims" (82% White, 57% female with a mean age of 46, and more likely to be in lower social grades, renters, and in urban areas); "elderly, vulnerable victims" (96% White, 74% female, had the highest mean age (69) of all clusters, and lower educational levels); "younger, high harm victims" (65% female, younger on average (41.6), and had a higher proportion of ethnic minorities (23%), and in urban areas).

Supporting victims of fraud

Reporting fraud and victim care

Rather than the police, victims of fraud are asked to report it to Action Fraud, the national reporting service.[2,34]

Victims may need to report the incident to their bank, building society or payment firm, which are responsible for reimbursement.[55,108]

Surveys generally show that: most frauds go unreported to Action Fraud or the police; [16,26,27,54,58,60,61] people are more likely to report frauds to relevant financial services; [16,26,54,58,60,61] and reporting rates vary for different types of fraud.[26,54,58–61] For example:

- Between April 2022 and March 2023, the CSEW found that 13% of fraud victims reported to the police or Action Fraud. Reporting rates were 9% for bank and credit account fraud, 15% for consumer and retail fraud, and 24% for other frauds.[54]

- The 2022 Financial Lives Survey[a] found that 87% of victims of debit or credit card fraud reported the crime to their account provider, 15% to Action Fraud and 6% to the police. For APP fraud, 61% of victims reported it to their account provider, 21% to Action Fraud and 10% to the police.[60]

In surveys of fraud victims, common reasons for not reporting frauds to official bodies include:

- thinking that reporting would not help or make any difference[26,27,38,54,58,59,61]

- not knowing how to report or who to tell[26,27,38,54,58,59,61]

- feeling it was not worth reporting, including that the fraud did not significantly affect them[26,27,54,58,59,61]

- feeling ashamed or embarrassed, or not wanting other people to know[26,38,54,58,59]

A range of organisations provide support and care for fraud victims in England and Wales (Box 2); arrangements and providers vary by area.[18,35,41,109]

Some research indicates mixed experiences for victims reporting crimes to authorities, for example in terms of being supported, their report being taken seriously, or expectations around their case being investigated.[16,98,103,110,111]

In the Crest Advisory survey, 73% of online fraud victims who reported to an official body said they had "very good" or "good" experiences with reporting, enforcement and outcomes, 18% "satisfactory" and 8% "not very good" or "awful".[26] Some

[a] The Financial Conduct Authority runs the Financial Lives survey, a nationally representative tracking survey of UK adults. The 2022 sample was based on 19,145 interviews taking place during February-June 2022 (18,889 online and 256 by telephone).

stakeholders refer to an element of 'victim-blaming' in reporting processes that can compound victims' own sense of shame.[16,61,91]

The 2023 Fraud Strategy (Figure 1) has a specific aim to improve consistency of victim care, including through replacing Action Fraud, expanding NECVCU, and extending the National Trading Standards multi-agency approach across England and Wales.[1]

Box 2: Victim care providers in England and Wales

Dedicated victim support services, which can provide practical, technical and emotional support, crime prevention advice, and signposting to other services, include:

- the **National Economic Crime Victim Care Unit (NECVCU)**, which supports fraud and cybercrime victims referred by Action Fraud[a] [33,35]
- **local police forces,** for victims of frauds they are investigating[1,35,37]
- **Victim Support**, which supports people affected by crime in England and Wales, and often works in conjunction with local forces[39,103]

Other agencies, providing more general support and advice, include:

- **local health and care services**, such as adult social care or community health services[40]
- **third sector** bodies such as Citizens Advice Bureaux and Age UK[43,44]

The **National Trading Standards Scams Team** provides guidance and best practice to assist local authorities and local multi-agency approaches in supporting victims.[16]

Reimbursement

Victims of unauthorised card fraud are legally protected against losses, with over 98% of customers fully reimbursed in 2022.[55] For victims of APP frauds, reimbursement depends on the policy of the financial provider, ranging from automatic reimbursement to limited eligibility.[57]

The 2023 Fraud Strategy has a specific aim to reimburse more victims.[1,5] From October 2024, the Payment Systems Regulator is due to introduce new rules on mandatory reimbursement for victims of APP frauds (Figure 1).[52]

By 2024, ten payment service providers (covering 90% of payments made) had signed up to the voluntary Contingent Reimbursement Model (CRM) code,[112,113] where

[a] Between April 2022 and March 2023, NECVCU supported over 113,000 victims.[33]

firms commit to reimburse victims of APP frauds if the customer has met certain standards.[a] [55,91,114]

UK Finance reported that 66% of APP losses were reimbursed under the CRM code in 2022.[55] In 2022, the Payment Systems Regulator noted inconsistent outcomes for victims of APP fraud across different payment providers, with the percentage of total APP fraud losses reimbursed ranging between 10%-91%.[57]

Future policy implementation considerations for victim support

Since 2022, three Parliamentary committees[b] have highlighted inadequacies in support for fraud victims including:[c] [28,29,109]

- unclear routes to report frauds and access support
- gaps and inconsistencies in provision of victim support
- poor service and information provision from Action Fraud

Some academic and financial sector stakeholders noted improvements in services for fraud victims (such as better training of bank staff and improved communications).[13,18,115,116]

Inspection and regulation bodies have highlighted remaining areas for improvement, including:

- **policing:** addressing the gap between the workload created by fraud and the available resources[20]
- **financial service providers:** supporting and identifying vulnerable customers; clear and timely communications; clear rationale for reimbursement decisions and consistent interpretation of customer responsibilities[115,116]

Stakeholders emphasise that effective victim support should be defined both in terms of reducing harm to victims and their risk of future victimisation.[11,35] However, given the low level of reporting, it is not known how many victims do not access support.[9,11]

The evidence base for effective support of fraud victims is very limited, compared to other crimes like burglary and violence.[9–15]

---

[a] For example, the customer must not have ignored warning messages from the bank and should have a reasonable basis for believing the payment is genuine.

[b] In 2022, House of Commons Justice Committee report Fraud and the Justice System (2022) examined the ability of the Justice System to effectively prosecute fraud cases, while the House of Lords Fraud Act 2006 and Digital Fraud Committee report Fighting Fraud: breaking the chain considered the Fraud Act 2006 and digital fraud. The 2023 House of Commons Public Accounts Committee report Progress Combatting Fraud looked at the effectiveness of the government's activity to combat fraud.

[c] Law enforcement and victim support stakeholders raised similar concerns.[16,35,41,74,100]

However, stakeholders suggested factors that may influence the effectiveness of implementation, including:

- Using **supportive, non-judgemental and empathetic** approaches.[10,16,18,35,41,61] This includes awareness of the risk of victim-blaming, such as in the language used for communications.[16,35,104,117]
- A focus on rebuilding victims' **strengths**, including their self-esteem, resilience and ability to avoid future revictimisation.[10,12,16,18,35,98]
- **Practical and technical** support, [10,12,35,41] provided in a timely fashion,[98] such as for claiming reimbursement or to improve internet security.
- Services **tailored** to individuals and the type of fraud, for example, different offers of practical vs emotional support.[a] [16,35,98,116]
- Given the scale of fraud, the available resources and variation in how victims are affected, **identifying and prioritising** the most affected victims for support,[9,11,98,109] including repeat victims.[118,119]
- **Joint working** between different agencies such as providing support or sharing information.[16,18,35]
- Appropriate **training** for those providing services.[17–19,35,109]
- Opportunities for victims to **share experiences**.[18,41,61]

Preventing fraud

There is consensus across stakeholders that prevention is a central component to reducing fraud and its impact on individuals.[15,28,29,77,100,101,109,111,120–122]

Preventing fraud against individuals includes 'upstream' prevention,[b] [123] which disrupts the source of the fraud, and is generally invisible to potential victims.[c] [11] Examples include actions to prevent 'number spoofing'[d] [124] and blocks on fraudulent texts.[e] [125]

---

[a] For example, Thames Valley police produces specific materials for victims of romance fraud.[36]

[b] In 2022, UK Finance reported that bank actions prevented £1.2 billion in unauthorised fraud, equivalent to over 60% of fraud attempted.[55]

[c] The Fraud Strategy has a specific aim to block frauds at source, reducing the number of fraudulent communications reaching the public. It includes measures to incentivise industry action; regulate to prevent fraudsters misusing technology; better protect customers; and secure people online at scale.[1]

[d] Number spoofing is where fraudsters appear to be calling from a legitimate phone number. In April 2019, HMRC introduced new controls, created in partnership with the telecommunications industry and Ofcom, to prevent 'spoofing' of its legitimate helpline numbers. The number of such calls reduced to zero following the new controls.[124]

[e] From April 2020, an online registry was introduced to help identify and block fraudulent texts, with a "significant drop" in such messages for customers of participating organisations.[125]

Other elements of prevention, which rely on individuals to take action in response to them, include:

- broader education campaigns (see Fraud education and awareness)
- 'midstream' prevention, which targets individuals at times of potential risk (see Fraud prevention targeted at moments of risk)[11]

There is consensus across different sectors that multiple elements of prevention are needed to reduce fraud, combining action from government bodies, law enforcement agencies, financial and online service providers, and individuals.[13,21,22,28,29,71,77,87,101–103,107,109,111,120–122,126]

Fraud education and awareness

In February 2024, the Home Office launched a national Stop! Think Fraud campaign in line with the Fraud Strategy.[a] [127,128] Previous fraud awareness campaigns include Take Five to Stop Fraud, run by UK Finance.[b] [129]

These campaigns aim to increase awareness of fraud and encourage individuals to take action to protect themselves.

Stakeholders note that the published evidence base for fraud education and awareness is very limited.[c] [10–12,14,19,21–23]

Future policy implementation considerations for fraud education

Stakeholders suggested challenges in implementing effective education and awareness campaigns:

- **Reaching those most at risk,** including: achieving a high overall reach;[d] [29,71] and identifying and reaching groups at higher risk of fraud and its impacts.[58,82,107] This also covers optimising communication channels and approaches to cover different groups and types of fraud.[9,14,61,78]

[a] The Stop! Think Fraud campaign has a key message of "Stay ahead of scams", with its website having sections on Are you at risk?; Protect yourself from fraud; How to spot fraud; Report fraud; and Recovery from Fraud. A prominent headline is: "Fraudsters aren't fussy. They'll pick on anyone."

[b] The Take Five to Stop Fraud campaign emphasises STOP (Taking a moment to stop and think before parting with your money or information could keep you safe), CHALLENGE (Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you) and PROTECT (Contact your bank immediately if you think you've been scammed and report it to Action Fraud).

[c] One as yet unpublished review noted positive findings for awareness-raising measures such as education campaigns, although dependent on context and delivery.[22]

[d] The National Crime Agency has reported findings from two surveys, which looked at awareness of the Take Five to Stop Fraud campaign. One survey of 2,079 adults found that 8% recognised the campaign. The other survey of 2,418 UK consumers found that 67% recognised Take Five or one of the STOP/CHALLENGE/PROTECT elements.[130]

- **Making campaigns relevant to a wide group of people,** including: engaging groups who may under-estimate their risk of victimisation;[14,41,82,83] not oversimplifying how easy it is to avoid being a victim;[16,23,41,78,83] and ensuring campaigns are effective for situations where fraudsters create relationships with victims.[11,104]

- **Using non-judgemental language:** stakeholders highlight the need to avoid "blaming/shaming" language (terms such as "scam" and "fall for")[a] and place responsibility on the fraudster rather than the victim.[14,16,23,41,83,87,131] UK Finance notes that people prefer more positive language, setting out what action they could take.[15]

- **Responding to the dynamic nature of fraud,** so campaigns remain relevant as frauds change.[10,13,14,19,81,107] Some bodies issue specific alerts for new frauds, alongside general warnings.[132]

- **Recognising the possibility that one fraud can cross over into a different type:** for example, a romance fraud developing into investment fraud.[16,78,133,134]

- **Providing information for supporting services,** such as guidance for staff and volunteers in contact with fraud victims and potential victims.[22,40,107]

Fraud prevention targeted at moments of risk ('midstream')

The published evidence base for 'midstream' fraud prevention is incomplete.[b9–12,16–18,20]

There are emerging and positive findings for specific interventions, such as call blockers and some industry interventions (Table 3).

Some stakeholders highlight the need for individuals to protect themselves against fraud.[18,86] Studies show that most people take active steps to protect their card and account details, personal information, and security online.[54,62]

In the 2022 Financial Lives Survey, 62% of adults said they (always or sometimes) took precautions to protect themselves against fraud (such as disposing of statements securely and covering their PIN). Those least likely to take precautions

[a] For example, UK Finance suggested referring to fraudsters as "criminals", and to people being "defrauded".[15]

[b] One unpublished review noted limited evidence of effectiveness for crime prevention based on non-technological methods (for example, spyholes, leaflets, junk mail blockers) or technological approaches (such as video door bells, warning lists, additional account monitoring, spam detectors or website fraud ratings).[22]

included those aged 18-24 and 75 or over, those with low financial capability and those in low-income households.[a] [60]

Table 1 Examples of fraud prevention initiatives and supporting evidence

Initiatives	Supporting evidence
Warning messages during payment transactions - extra messages when customers set up, change or make payments.[114] 'Call to action' (CTA) buttons can also be shown during transactions, which make it easier for customers to cancel or defer transactions.	• In 2023, UK Finance reported a 35% reduction in frauds involving impersonation of financial services firms, following the introduction of new warning messages.[64] • A 2021 online experiment found that including CTA buttons could reduce fraud: 10% of CTA users made fraudulent payments compared to 22% in the control group. The largest effect was found for CTA buttons combined with risk-based warnings; risk-based warnings alone did not appear to have an impact. However, including CTA buttons also made customers less likely to complete a genuine payment.[135]
Confirmation of Payee (CoP) - customers setting up a new payee are asked to confirm that the name they have entered matches the one on the account they intend to pay, and alerted to whether there has been a match, a close match, or no match.[46]	• In 2020, Lloyds Bank reported that APP frauds had fallen by 31% among customers who had used CoP.[136] In 2021, the Payment Systems Regulator (PSR) reported data analysis that suggested a reduction in relevant frauds for payment service providers using CoP, compared to an increase for providers not using CoP.[137] • PSR also reported that fraudsters were already developing techniques against the CoP checks (for example, by manipulating people into bypassing checks).[137] • CoP relies on customers taking action if they are alerted to non-matches.[60] In 2022, Lloyds Bank reported that 8% of account holders said that they had proceeded with a payment and not made further checks when CoP indicated there was not an exact match.[138]
Call blockers plug into existing phones/phone lines and filter out unwanted calls. Users can identify trusted callers, such as friends and family.	An evaluation for National Trading Standards[139] of over 1,000 call blockers installed during 2019-20 found that they: • Were effective in preventing fraud, blocking over 99% of scam and nuisance calls. Before installation, 94% of respondents received scam or nuisance phone calls in the previous 6 months; 3 months after installation, 92% of respondents reported not receiving any scams or nuisance calls.[106] • Improved wellbeing, especially for older people, vulnerable individuals and those living alone. 96% of applicants reported a positive impact on their wellbeing, 3 months after installation.[106]

[a] The Financial Lives Survey measure of 'financial capability' was based on respondents' self-ratings of their confidence in managing money, and knowledge about financial matters, and whether they agreed or disagreed with the statement 'When it comes to financial services and products, I would consider myself to be a confident and savvy consumer'. Low-income households were defined as those earning less than £15,000.

Future policy implementation considerations for fraud prevention

Stakeholders suggested potential considerations for effective prevention, including:

- The use of **dynamic** prevention approaches, which can:
  - keep up with the changing nature of fraud.[11,91,120,140]
  - be tailored to different consumers, transactions, frauds, and stages in the payment process, to engage people to take action.[91,120,140]
- How prevention works for **vulnerable groups,** including:
  - providing tailored support, for example, extra checks on transactions, or introducing pauses into the payment process.[18,86,107,115,116,139]
  - identifying vulnerable customers.[115,116]
- Awareness of **potential trade-offs and unintended consequences** of preventive measures.[11] For example, some interventions may deter people from making a genuine payment[135] or isolate individuals.[12] The Lending Standards Board states that firms are balancing the introduction of effective warnings into the payment process while minimising inconvenience.[140] Research suggests that consumers may be more open to additional checks than data sharing:
  - A poll of more than 2,000 UK adults for the Social Market Foundation showed 70% support more stringent checks on payments and transfers over convenience and speed, if it reduced fraud risk. A lower proportion favour more data sharing within the private sector (31%) or for law enforcement purposes (36%) to reduce fraud risk over strong privacy/data security.[96]
  - The 2022 Financial Lives Survey found that only 5% of consumers mind the extra time that it takes to make payments following the introduction of Strong Customer Authentication.[a 60]

[a] Strong Customer Authentication is used by banks and payment services providers to verify a customer's identity when making an electronic payment or accessing their account, generally through a text message, email, or app on a mobile device.

References

1. Home Office (2023). Fraud Strategy: stopping scams and protecting the public. *GOV.UK*.
2. Office for National Statistics (2023). User guide to crime statistics for England and Wales: March 2023.
3. Office for National Statistics (2024). Crime in England and Wales: year ending September 2023. Office for National Statistics.
4. Office For National Statistics (2024). Crime in England and Wales: Appendix tables.
5. Home Office (2023). Fraud Strategy. *GOV.UK*.
6. Ofcom (2023). Ofcom's approach to implementing the Online Safety Act. *Ofcom*.
7. legislation.gov.uk (2023). Online Safety Act 2023. Explanatory notes.
8. Home Office (2023). Online Fraud Charter.
9. Levi, M. (2023). Human, political and technological factors involved in a public health approach to fraud. *Human Factors in Cybercrime Conference, Halle*,
10. Correia Hopkins, S. (2024). Personal communication.
11. Levi, P. M. (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0088). Home Affairs Committee, House of Commons, UK Parliament.
12. Lea, S. (2023). Personal communication (interview).
13. Button, M. (2023). Personal communication (interview).
14. UK Finance (2023). Personal communication.
15. UK Finance (2023). Personal communication.
16. National Trading Standards Scams Team (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0041). Home Affairs Committee, House of Commons, UK Parliament.
17. Which? *et al.* (2022). The Psychology of Scams. Which?
18. Carter, E. (2024). Personal communication.
19. Which? (2023). Personal communication.
20. Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (2021). Spotlight report - A review of Fraud: Time to Choose.
21. Levi, M. (2023). Personal communication.
22. Button, M. (2023). Personal communication (unpublished research).
23. Chartered Trading Standards Institute (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0047).
24. Action Fraud (2021). 2020-21 Annual Assessment Fraud Crime Trends.
25. Office of the City Remembrancer on behalf of the City of London Police and City of London Police Authority Board (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0092).
26. Reynoso-Serna, F. *et al.* (2023). Online fraud: what does the public think? Crest Advisory.
27. Blakeborough, L. *et al.* (2018). The scale and nature of fraud: a review of the evidence. Home Office.
28. Fraud Act 2006 and Digital Fraud Committee (2022). Fighting Fraud: Breaking the Chain. House of Lords.
29. House of Commons Committee of Public Accounts (2023). Progress combatting fraud.
30. Ofcom (2022). Tackling scam calls and texts: Ofcom's role and approach.
31. BT Group (2024). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA099).
32. Meta (2024). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0100).

33. City of London Police (2023). Specialist victim care unit which supports thousands of vulnerable fraud victims rolled out across the UK.
34. Police.uk Action Fraud.
35. NECVCU (2024). Personal communication.
36. Thames Valley Police A guide to spotting romance fraudsters.
37. City of London Police (2023). National Policing Strategy for Fraud, Economic and Cyber Crime 2023 – 2028.
38. National Crime Agency (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0077).
39. Victim Support Fraud. *Victim Support*.
40. Brown, K. *et al.* (2020). Scams: the Power of Persuasive Language. Guidance for community health and social care workers to help identify and prevent scams in society. Bournemouth University / The National Centre for Post-Qualifying Social Work and Professional Practice.
41. Victim Support (2023). Personal communication.
42. Which? Scams - Which? Consumer Rights. *Which?*.
43. Age UK Scams advice – How to spot and avoid scams. *Age UK*.
44. Citizens Advice Get help with scams. *Citizens Advice*.
45. National Trading Standards About National Trading Standards - National Trading Standards.
46. Payment Systems Regulator (2023). APP scams.
47. OfCom (2023). What is Ofcom? *Ofcom*.
48. Financial Conduct Authority (2016). Fraud. *FCA*.
49. Lending Standards Board About the LSB.
50. OfCom (2023). Protecting people from illegal harms online. Volume 1: Background to the new Online Safety regime (introduction, illegal content duties and offences, and overview of regulated services).
51. Cavaglieri, C. (2023). New rules for bank transfer fraud reimbursement from 2024. *Which?*.
52. Payment Systems Regulator (2023). PS23/4: APP scams reimbursement policy statement.
53. legislation.gov.uk (2006). Explanatory Notes to Fraud Act 2006. King's Printer of Acts of Parliament.
54. Office for National Statistics (2023). Nature of fraud and computer misuse in England and Wales: appendix tables.
55. UK Finance (2023). Annual Fraud Report. The definitive overview of payment industry fraud in 2022.
56. Ramsey, T. (2022). Notorious 'Hi Mum and Dad' scam spreads from WhatsApp to text message - Which? News. *Which?*.
57. Payment Systems Regulator (2023). Authorised Push Payment (APP) fraud performance report - October 2023.
58. European Commission (2020). SURVEY ON "SCAMS AND FRAUD EXPERIENCED BY CONSUMERS". European Commission.
59. Yonder Consulting (2023). Executive Summary Report: Online Scams & Fraud Research. Ofcom.
60. Financial Conduct Authority (2023). Financial Lives 2022 survey - Key findings from the May 2022 survey: Executive summary.
61. Futuresight (2020). Communications Networks and Fraudulent Activity Research Report of Findings. Communications Consumer Panel.
62. Transunion (2023). TransUnion Consumer Pulse Report Q4 2023.
63. Office for National Statistics (2022). Nature of fraud and computer misuse in England and Wales.
64. UK Finance (2023). 2023 Half Year Fraud Update. UK Finance.
65. Lloyds Banking Group (2023). Two-thirds of all online shopping scams

now start on Facebook and Instagram.
66. Office for National Statistics Nature of crime: fraud and computer misuse - tables.
67. Citizens Advice What you can do with your pension pot. *Citizens Advice*.
68. NHS Counter Fraud Authority COVID-19 vaccine fraud.
69. TSB (2024). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0102).
70. Clean up the Internet (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0024).
71. Hyde, R. Fraudulent times: Identifying a consensus for an agenda to beat fraud. Social Market Foundation.
72. GOV.UK Recognise the tactics (Stop! Think Fraud). *Stop! Think Fraud*.
73. Building Societies Association (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0039).
74. Greater Manchester Office for Police Crime Commissioner *et al.* (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0035).
75. Barclays Bank (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0025).
76. Lloyds Banking Group (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0054).
77. The Payments Association (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0079).
78. Kassem, R. *et al.* (2023). Mapping Romance Fraud Research – A Systematic Review. *Journal of Financial Crime*,
79. Home Office (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0080).
80. UK Finance About us. *UK Finance*.
81. Lea, S. (2023). Personal communication (unpublished research).
82. Norris, G. *et al.* (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *J Police Crim Psych*, Vol 34, 231–245.
83. Carter, E. (2023). Confirm Not Command: Examining Fraudsters' Use of Language to Compel Victim Compliance in Their Own Exploitation. *The British Journal of Criminology*, Vol 63, 1405–1422.
84. Carter, E. (2021). Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud. *The British Journal of Criminology*, Vol 61, 283–302.
85. Centre for Economic Performance at the London School of Economics (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0083).
86. National Trading Standards Scams Team (2023). Personal communication.
87. Kassem, R. (2023). Personal communication.
88. Poppleton, S. *et al.* (2021). Who suffers fraud? Understanding the fraud victim landscape. Victims Commissioner.
89. Briody, L. (2021). Policing and Vulnerability: who is vulnerable?
90. National Residential Landlords Association Avoiding Fake Landlord Scams | NRLA.
91. Cavaglieri, C. (2020). Banks denying refunds to scam victims who ignore new warnings - Which? News. *Which?*.
92. Lloyds Banking Group (2020). On The Fraudline Lloyds Bank Calls On Brits To Join The Fight Against Fraud By Kickstarting Conversations On Scam Spotting.
93. Button, M. *et al.* (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Secur J*, Vol 27, 36–54.

94. Kassem, R. (2023). How fraud impacts individuals' wellbeing – academic insights and gaps. *Journal of Financial Crime*, Vol ahead-of-print,
95. Ofcom Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers. Ofcom.
96. Hyde, R. *et al.* The view from the ground: Building a greater understanding of the impact of fraud and how the public view what policymakers should do about it. Social Market Foundation.
97. Home Affairs Committee [@CommonsHomeAffs] (2024). Twitter post (survey findings). *Twitter*.
98. Home Office (2024). Personal communication (forthcoming research publication).
99. Office for National Statistics (2023). Crime in England and Wales: Other related tables.
100. Office of the West Midlands Police and Crime Commissioner (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0086).
101. TSB (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0081).
102. Communications Consumer Panel (2020). Scammed! Exploited and afraid. What more can be done to protect communications consumers? (2020).
103. Victim Support (2023). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0026).
104. Hawkswood, J. *et al.* (2022). Coercion and control in financial abuse; learning from domestic abuse. National Trading Standards Scams Team.
105. OfCom (2023). Online Nation - 2023 Report.
106. Rosenorn-Lanng, E. *et al.* (2020). Exploring the Impact of Call Blockers on User Well-Being. Bournemouth University, National Trading Standards Scams Team.
107. Re-engage (2023). The unseen price of a scam: The impact of scams and fraud on isolated older people.
108. Payment Systems Regulator PS23/3: Fighting authorised push payment fraud: a new reimbursement requirement.
109. Justice Committee (2022). Fraud and the Justice System.
110. Dinisman, T. *et al.* (2017). Understanding victims of crime. Victim Support.
111. Police Foundation Written evidence submitted to the Home Affairs Fraud inquiry (FRA0011).
112. Lending Standards Board (2022). Written evidence submitted to the House of Lords Committee on the Fraud Act 2006 and Digital Fraud (FDF0050). UK Parliament.
113. Lending Standards Board (2023). The Contingent Reimbursement Model Code (CRM Code).
114. Lending Standards Board Information for customers on the Contingent Reimbursement Model Code for APP scams (the CRM Code).
115. Lending Standards Board (2023). Summary Report: Customer Vulnerability.
116. Lending Standards Board (2022). 2022 Review of adherence to Contingent Reimbursement Model Code for Authorised Push Payment Scams.
117. Cross, C. (2018). Denying victim status to online fraud victims: the challenges of being a 'non-ideal victim'. in *Revisiting the "Ideal Victim": Developments in Critical Victimology*. (ed. Duggan, M.) 0. Policy Press.
118. Correia, S. (2021). Vulnerability and Repeat Victimisation in a Digital World: A Study of Computer Misuse and Fraud Reported in Wales.
119. Correia, S. G. (2019). Responding to victimisation in a digital world: a

case study of fraud and computer misuse reported in Wales. *Crime Science*, Vol 8, 4.
120. Bamber, O. (2021). The power of prevention in the fight against APP fraud. *Lending Standards Board*.
121. Stop Scams UK (2023). Written evidence submitted to the Home Affairs Fraud inquiry (FRA0093).
122. Innovate Finance (2024). Written evidence submitted to the Home Affairs Fraud Inquiry (FRA0098).
123. Coote, A. The Wisdom of Prevention. *New Economics Foundation*.
124. HMRC (2019). Controls prevent phone fraudsters spoofing HMRC. *GOV.UK*.
125. Mobile Ecosystem Forum SMS SenderID Protection Registry. *MEF*.
126. OfCom (2023). Personal communication.
127. Home Office Major campaign to fight fraud launched. *GOV.UK*.
128. GOV.UK Stop! Think Fraud. *Stop! Think Fraud*.
129. UK Finance About Take Five. *Take Five*.
130. Biggar, G. *et al.* (2022). Progress combatting fraud inquiry - additional evidence from the National Crime Agency - submission to Public Accounts Committee.
131. North East Regional Cyber Crime Unit (2023). SCAM - What does the word mean to you? *North East Regional Economic and Cyber Crime Units*.
132. Which? (2024). The latest scam alerts from Which? - Which? News. *Which?*.
133. Carter, E. (2024). The Language of Romance Crimes: Interactions of Love, Money, and Threat. *Elements in Forensic Linguistics*, Cambridge University Press.
134. Whittaker, J. M. *et al.* (2024). Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology*, Vol 3, 100052.
135. The Behaviouralist (2021). Redesigning online banking environments to reduce fraud.
136. Nixon, G. (2020). Name-checking Confirmation of Payee cuts bank scams 31%, says Lloyds. *This is Money*.
137. Payment Systems Regulator (2021). CP21/6 - Confirmation of Payee - Phase 2 Call for Views.
138. Lloyds Banking Group (2022). Millions of Brits at greater risk of fraud after ignoring vital bank payment warnings.
139. National Trading Standards Scams Team (2021). Call Blocking 2019-2020. National Trading Standards.
140. Lending Standards Board (2020). Thematic review of provision SF1(2) – Effective warnings. Summary Report.

Contributors

For further information on this subject, please contact Natalie Low or Clare Lally. POST would like to thank interviewees and peer reviewers for kindly giving up their time during the preparation of this briefing, including:

Members of the POST Board*

Home Office*

Financial Conduct Authority

National Economic Crime Victim Care Unit (NECVCU)*

Louise Baxter Scott, National Trading Standards Scams Team*

Professor Mark Button, University of Portsmouth

Dr Elisabeth Carter, Kingston University*

Dr Sara Correia-Hopkins, University of Swansea

Matt Gardner and Tim Stacey, Which?*

Paul Jacobus, Ofcom

Dr Rasha Kassem, Aston University*

Emeritus Professor Stephen Lea, University of Exeter*

Professor Michael Levi, Cardiff University*

Paul Maskall, UK Finance

Giles Mason and Sarah Sinden, UK Finance

Alex Mayes, Victim Support

The Parliamentary Office of Science and Technology (POST) is an office of both Houses of Parliament. It produces impartial briefings designed to make research evidence accessible to the UK Parliament. Stakeholders contribute to and review POSTnotes. POST is grateful to these contributors.

If you have any comments on our briefings please email papers@parliament.uk. Please note that we are not always able to engage in discussions with members of the public who express opinions about the content of our research, although we will carefully consider and correct any factual errors.

If you have general questions about the work of the House of Commons email hcenquiries@parliament.uk or the House of Lords email hlinfo@parliament.uk.

DOI: https://doi.org/10.58248/PN720

Image Credit: Photo by rupixen on Unsplash

post@parliament.uk
parliament.uk/post
@POST_UK