# Generation Fraud: Is social sharing putting younger generations at risk?

*An analysis of how people aged under 35 are particularly at risk from fraud, with original research and expert views on the growing threats from AI and deepfakes.*

finder.com

# Introduction



Fraud, including ID theft, accounts for 40% of UK crime, according to the most recent figures from the Financial Conduct Authority (FCA). And it's a particular problem for younger generations who've grown up publicly sharing personal details online.

UK Finance reported in September 2023 that under-25s are more likely than older age groups to be targeted - 49% said they'd been contacted by an impersonation scammer vs 33% of over-55s. Over half the under-25s targeted said they shared personal information or made a payment as a result of the contact.

Younger generations are freer with their personal information but also less concerned than other age groups about fraud using artificial intelligence (AI), new research from Finder shows. In our survey of 2,003 adults, 35% in the 25-34 age group had publicly shared enough information to increase their risk of ID theft. But only 54% of gen Z (aged 18-23) and 60% of millennials (aged 24-42) were concerned about AI fraud, compared with 82% of those aged 74+.

A major challenge is how technology enables fraudsters to harvest information and commit more sophisticated crimes at scale. Being concerned - or risk-aware - is sensible. The tech is evolving fast and fraudsters will be working on more efficient and convincing clones and deepfakes.

So who should be doing more to tackle fraud? 86% of Brits believe more should be done, but opinions vary over who should do it. Just over half (51%) believe the list includes the government. But similar percentages also think the FCA, police, banks, and social media companies should do more (see p8).

The new Economic Crime and Corporate Transparency Act 2023 made "failure to prevent fraud" a corporate criminal offence. But its impact is still unclear.

To better understand trends and the challenges in tackling the problem, we asked 6 industry experts their views. Read their insights and predictions alongside our exclusive research in this report.

## Contents



Any content from this paper, including illustrations, may be freely reproduced as long as the source is cited with a link to https://www.finder.com/uk/improve-your-credit-score#fraudreport

# Expert panel



### Iona Bain, finance journalist and broadcaster

Iona is an award-winning journalist, broadcaster, speaker and author. She is *BBC Morning Live's* resident financial expert. Iona was commissioned by BBC Radio 4 to investigate the world of fraud for its *The Anatomy of a Fraud* programme, broadcast in 2023.

### Paul Evans, fraud expert, Featurespace

Paul has 18 years' experience of protecting high street banking customers from becoming victims of fraud by detecting and preventing fraudsters' attempts to steal their money. He currently works at Featurespace, a leading global supplier of fraud detection software for financial institutions.

### Mike Harlock, senior financial crime manager, Moneybox

Mike works in the Risk & Compliance team at Moneybox, a wealth management app that helps people "turn their money into something greater", such as helping them buy their first home, invest for the future or save for retirement. Mike has over 17 years' experience in regulatory compliance and financial crime prevention.

### Ebru Keskin, lecturer and consultant in payments and fraud

Ebru is an online payments and fraud prevention expert with over 12 years' experience at enterprise level. She's worked and consulted with some of the world's most prominent enterprises. Ebru has developed and is interested in improving artificial intelligence software and the machine learning which powers it.

### John Somerville, director of financial services, London Institute of Banking and Finance

John has over 30 years of experience in financial services and now plays an active role educating others as a spokesperson for the London Institute of Banking and Finance, which provides finance industry qualifications in the UK.

### Erica Stanford, author and lecturer

A fintech and AI specialist, Erica wrote *Crypto Wars: Faked Deaths*, *Missing Billions* and *Industry Disruption*, which was highly commended in the Business Book Awards. She speaks and writes globally about digital assets, scams, and the integration of AI, and is an associate guest lecturer on digital assets at Warwick Business School. Erica founded the Crypto Curry Club, a leading crypto community.

Any content from this paper, including illustrations, may be freely reproduced as long as the source is cited with a link to https://www.finder.com/uk/improve-your-credit-score#fraudreport

# What are the biggest challenges in tackling fraud in the UK?



### Paul Evans, Featurespace

Scams are the main type of fraud people are losing money to right now in the UK. The big challenge with tackling scams is reliance on the victim spotting or accepting that the scam is in progress when they are warned. Scams involve very strong emotional manipulation that needs to be unpicked and reversed through warnings and conversations with customers and this is very difficult to do. Banks work hard to educate customers…and implement detection so that they can warn customers as the scam is happening.

### John Somerville, London Institute of Banking and Finance

The increasing sophistication of cybercriminals poses a significant challenge. Phishing attacks, ransomware, and other forms of online fraud continue to evolve, making it difficult to stay ahead of cyber threats.

### Erica Stanford, author and lecturer

The main new challenge is the rapid technological advancements outpacing any attempts at tackling fraud. AI deepfakes - voice cloning and video manipulation, and photos, audios and written texts that are now indistinguishable from the person or entity they are imitating - are one. Law enforcement have limited resources, and so have to choose which fraud…they go after, typically only having the resources to go after those frauds with the highest chance of conviction and that will net them the highest gains.

### Mike Harlock, Moneybox

One of the biggest challenges is a lack of specialist fraud knowledge in some areas of law enforcement, which can make it difficult to report fraud, especially for some…lower level fraud... Fraud is now the most common type of crime in England and Wales, but the specialist knowledge on this is still far too concentrated. The other big challenge is information sharing between businesses; very often each will only see a small part of the picture, and there is still a lot of hesitancy among firms to share information with each other.

> The lack of regulation of tech platforms has allowed certain scams to flourish. Now scams [are] popping up on all social media platforms (and through search engines) there can be an infinite number of scams and…a potentially limitless number of victims.
>
> *Iona Bain, finance journalist and broadcaster*

Any content from this paper, including illustrations, may be freely reproduced as long as the source is cited with a link to https://www.finder.com/uk/improve-your-credit-score#fraudreport

### Erica Stanford, author and lecturer

I expect AI to bring about an increased number of frauds, and frauds that are more sophisticated and harder to detect. [But] AI…will bring about enhanced abilities in fraud detection [and] allow companies, social platforms and law enforcement to process larger datasets faster to identify and respond to fraudulent activities. Tools such as transaction monitoring, identity verification, and claims analysis are already quickly becoming more advanced, and [may] catch up with the new types of fraud.

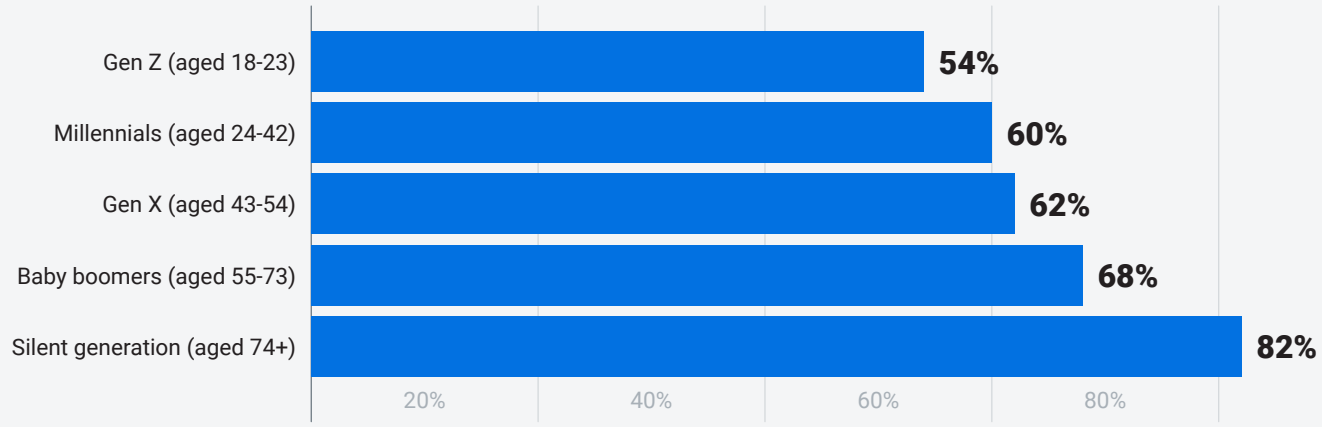
### Mike Harlock, Moneybox

AI is going to be just as disruptive to the illegal economy as it will to the legitimate economy. As with any new and emerging technology, fraudsters will be at the forefront of trying to use AI for their own means, whether…using ChatGTP to write scam emails or using AI to generate fake and synthetic identities. The use of deepfakes to commit identity fraud is a big concern; celebrity deepfakes will always grab the headlines, but as the software…becomes more available and scalable, we could see a big rise in this type of fraud. And some of the examples I've seen are really convincing and stand up to scrutiny. Fake identities used to access the financial system make it easier for the proceeds of crime to be moved around.

### Paul Evans, Featurespace

AI can impact both sides of fraud. Banks have been using it for years to detect and prevent fraud and now…fraudsters are using it as well. There are regularly new variations of fraud emerging, but they often come back to similar themes of technical compromise such as malware and hacking, information compromise, such as phishing, and then consumer compromise where the consumer…is making the payment that is fraudulent. Using generative AI to profile a person's transactions and then predict future transactions is new and is expected to be a game changer…in detecting fraud. It is expected to be more flexible and more powerful than other existing AI approaches and therefore prevent more fraud in the longer term.

## How many in each generation are concerned about fraud using AI?




Source: Finder survey, November 2023

Any content from this paper, including illustrations, may be freely reproduced as long as the source is cited with a link to https://www.finder.com/uk/improve-your-credit-score#fraudreport

# What are the trends in fraud that targets individuals?



### Paul Evans, Featurespace

More people are being targeted across more communication channels…email, phone, SMS, messaging apps, social media adverts, internet advertising, app stores and marketplaces. All of these have fraud elements…where fraudsters attempt to trick people into giving out information or sending them money. The old advice still applies of "If it is too good to be true then it probably is," but we need to go further and be wary of all communication and look for a way of verifying who it is from and [whether it is] true.

### Mike Harlock, Moneybox

Increasingly investment scams are offering higher…returns, which should act as a red flag for people, but sadly against the backdrop of increasing living costs these prove all too tempting. Recent reports from UK Finance and the National Crime Agency have highlighted how money muling remains a top concern, as mules are being used to handle the proceeds of fraud. Historically, young people and students have been recruited as money mules, so it's important that we educate those that could be susceptible to falling for this type of activity.

### Erica Stanford, author and lecturer

I have seen a huge rise in social engineering crimes. Here, users are sent emails or messages or calls from their “bank” that look real. Authorised push payment fraud is also on the rise. Here, victims are tricked into authorising payments to accounts controlled by fraudsters, typically again using social engineering tactics. The weaker economy and cost of living crisis create increased levels of vulnerability, with more vulnerable people prone to falling victim to scams.

### Iona Bain, finance journalist and broadcaster

The tactics fraudsters will use when they’re engaging in push payment fraud will relate to…”social engineering”. This is basically the use of very clever psychological tactics to disarm and charm the person they’re trying to defraud.

### Case study: Fraudsters threatening arrest coerced Tash into £1,900 transfer

Tash, aged 24, is a PR exec in London. In July 2022, she got a call from an unknown number, from someone claiming to be from HMRC.

"They knew my name and asked me to confirm my date of birth and address. They said someone had used my details to transfer a large amount of money abroad, and offences had been committed which were in my name. I wanted to call my mum but they said if I hung up, it would show I wasn't co-operating and I'd be arrested.

"I was on the phone for an hour and they persuaded me to download an app which allowed them to see my phone screen. They coerced me into sending £1,900 to avoid my assets being frozen. They said I’d get it back. They could see my bank details. I walked to a police station and they hung up. The banks were really good and I got my money back a month later.”

Any content from this paper, including illustrations, may be freely reproduced as long as the source is cited with a link to https://www.finder.com/uk/improve-your-credit-score#fraudreport

# Are you concerned about those who grew up sharing on social media?



### Iona Bain, finance journalist and broadcaster

My main concern is that they're growing up as digital natives, and using social media platforms every day. They may not be aware or informed about what a scam looks like. I think young people don't necessarily understand that when they're putting their pet's name on social media, or sharing their address, or even just sharing their location...they are actually putting a lot of information out there that fraudsters could use to try to access their financial details and to therefore successfully perpetrate identity fraud.

### John Somerville, London Institute of Banking and Finance

My first concern is that younger individuals who are active on social media...may be more susceptible to social engineering attacks. Cybercriminals can exploit the personal information shared online to craft convincing phishing messages or engage in other manipulative tactics. [My second is] scams targeting individuals through social media platforms that may involve fake investment opportunities, phishing links, or requests for personal information under the guise of a trusted entity. And thirdly, lack of financial literacy can make them more vulnerable because [a] limited understanding of financial concepts can result in poor decision-making regarding money matters.

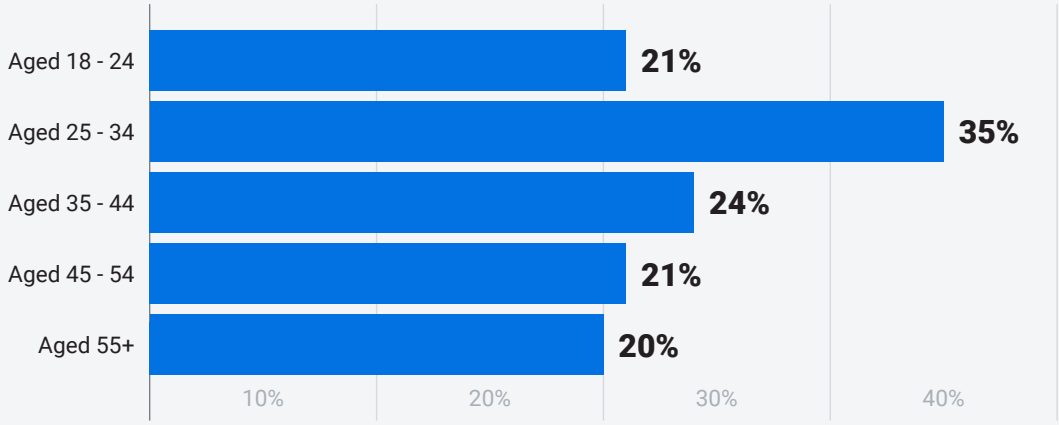
### Erica Stanford, author and lecturer

The more people use social media, the more personal details they will normally give away, with often no idea of how these details can be used against them.

### Mike Harlock, Moneybox

Gen Z and younger are so used to living their lives online, that sharing information is second nature to them. I would be very worried that they could be more susceptible to online scams and fraud. Even if they don't actively fall for phishing scams, there is so much information available about someone via social media, that it could be straightforward for a fraudster to steal their identity or at least target them via social engineering attacks. Research has also shown that Gen Z could be more susceptible to falling for impersonation scams as they are so used to managing their finances online or remotely.

## How many are at higher risk of fraud from sharing sensitive information?




Source: Finder survey, Nov 2023. Figures are those who publicly shared at least 2 pieces of personal information

Any content from this paper, including illustrations, may be freely reproduced as long as the source is cited with a link to https://www.finder.com/uk/improve-your-credit-score#fraudreport

# Who should tell young people the risks from sharing information?



### Mike Harlock, Moneybox

I see this very much as a collective responsibility. Banks, police and regulators already do a lot of educational activities here, such as Take Five and Scam Smart, so I think schools need to do much more. But then this applies to financial education in general, not just information sharing and fraud! There's already a lot of information about staying safe online for children and teenagers, although none of it really focuses on fraud.

### John Somerville, LIBF

I believe it needs to be a fully integrated system involving all parties. The approach needs to be joined up and focused on making the process of financial education consistent and in understandable language.

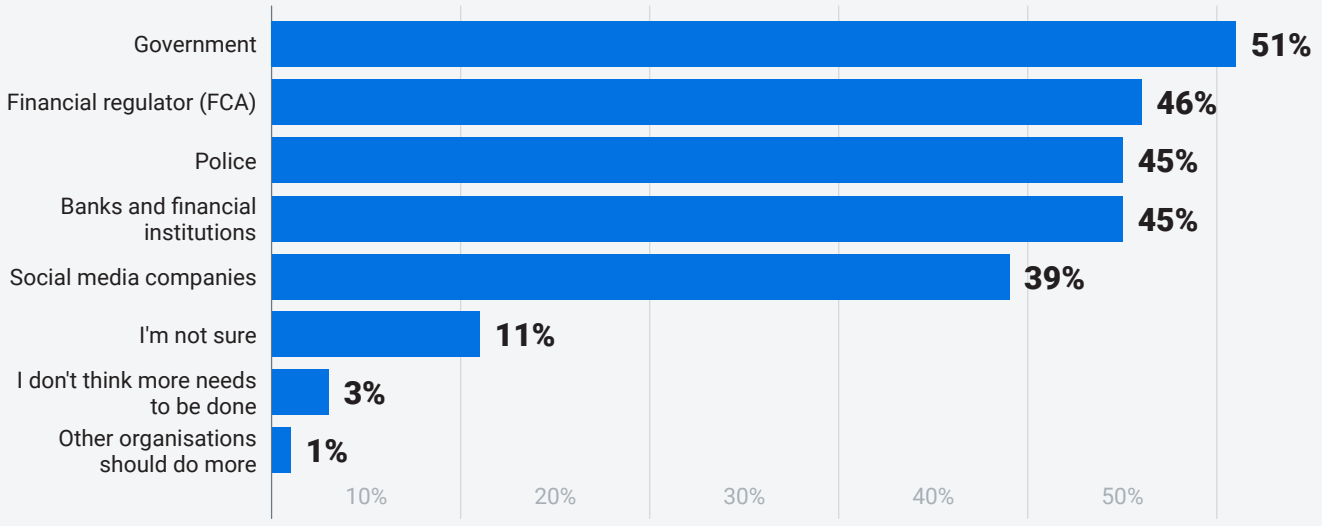
### Paul Evans, Featurespace

I think education needs to start as young as possible and school is therefore the best place for it, but ideally everyone in society takes some responsibility to protect and educate where they can and enable a greater impact. Regulators could do more to influence social media and manage content and hopefully we have seen a big first step towards this in the UK with the Online Safety Bill becoming law at the end of October 2023.

### Ebru Keskin, lecturer and consultant in payments and fraud

Parents [are responsible]. I think it's about making people aware that their personal finance is their responsibility. Banks also have to do a lot more. When they offer bank accounts that provide people with ways of paying online, they have to educate and explain what it means; they have a responsibility to explain to their younger clients they're not always safe. And also the device makers because they have to ensure payment security.

### Do you think more needs to be done to prevent ID fraud? If so, by whom?




Source: Finder survey, Nov 2023. Respondents could choose all relevant options

Any content from this paper, including illustrations, may be freely reproduced as long as the source is cited with a link to https://www.finder.com/uk/improve-your-credit-score#fraudreport

# What innovations are helping to protect customers?



### Erica Stanford, author and lecturer

Biometric logins help. The best I've seen offers a constant facial scan, ensuring only the authenticated user is the one making the transaction or in the field of communication at all times. AI and behavioural analytics tools are also advancing, but still prone to making mistakes.

### John Somerville, LIBF

My personal main 3 are: the use of biometric data - such as fingerprints, facial recognition, and voice recognition - becoming more widespread; multi-factor authentication (MFA), and behavioural biometrics which analyse user behaviour can help in identifying anomalies that may indicate fraudulent activity.

### Mike Harlock, Moneybox

Firms are using their own AI and machine learning tools to help spot suspicious transactions and fake identities, to keep their customers and themselves safe from bad actors. In some cases, regtech firms are starting to generate their own fake identities, and then using these to train their AI software on what to look out for, ensuring that they respond quickly to new typologies and attack vectors - all pretty innovative, using fraudsters' methods against them!

### Iona Bain, finance journalist and broadcaster

Banks are becoming much more aware of the dangers of AI and how it could be used to manipulate their security systems, and that means identity fraud will become an increasingly difficult crime to pull off. The security checks the banks do are pretty robust in preventing someone from posing as somebody else and the banks' education around fraud is getting better.

### Paul Evans, Featurespace

Trust and checking services are a fairly new innovation to protect customers. These services are similar in some ways to review sites, except they review more information from more angles to generate a confidence or risk score for consumers to use. The score could relate to a website and simply be whether the site is genuine or is likely to be phishing or another type of scam.

> A really helpful development is the phone line that's been established by the banking industry that customers can use...to check if someone contacting them is actually from their bank. If this is rolled out everywhere, and free, it could be a gamechanger.
>
> *Iona Bain, finance journalist and broadcaster*

Any content from this paper, including illustrations, may be freely reproduced as long as the source is cited with a link to https://www.finder.com/uk/improve-your-credit-score#fraudreport

### Erica Stanford, author and lecturer

I'm of the view…that we have no idea about the potential of AI, what AI already knows, and where it might be going. AI frauds will grow in range and sophistication. One risk, which I think is inevitable, is that AI will train itself to think of and create new types of frauds. Once it has created these, it will be able to train itself on how to make these be more successful, by analysing what works and what doesn't.

### Mike Harlock, Moneybox

I think as AI gets more advanced and more available, we'll see it used more and more to enable fraudulent activity and firms will need to up their own AI game to keep up! Not only will AI use rise among professional fraudsters, or those of "fraud as a service", but also in lower level ways as the software becomes more readily available.

### Paul Evans, Featurespace

Fraud will continue to attempt to expand, and fraud detection, driven by artificial intelligence, will continue to progress and force fraudsters to be more subtle and try to appear more legitimate. We will see improved algorithms predicting transactions and identifying suspicious behaviour as well as assessing and sharing information across sectors in a form of "digital ID" that can represent levels of risk and trust for payers and payees.

### John Somerville, LIBF

Predicting the future is inherently uncertain, but several trends and possibilities can be considered in the long-term linkage between fraud and AI. Here are some potential developments: increased sophistication of AI-based attacks, AI-enhanced fraud detection and prevention, biometric advancements, collaboration across industries, and a plan for AI ethics and regulation.

## Conclusion

While UK fraud losses fell slightly, to £580 million, in the first half of this year, authorised push payment (APP) fraud cases rose by 20% compared with the same period in 2022, according to UK Finance. And, 78% of APP fraud cases start online, compared to just 18% on the telephone. UK Finance says fraudsters are focusing on social engineering, to trick people into handing over personal details which are then used to target victims.

Sharing too many personal details online gives the criminals a head start. And Finder's research shows that people aged 25-34 in particular are putting themselves at higher risk through what they share publicly. Thanks to AI, impersonation scams are likely to get more sophisticated, too.

Under rules due in 2024, banks will be compelled to refund APP victims. Now could be an ideal time for more innovations in protection, and a major drive to raise awareness.

Any content from this paper, including illustrations, may be freely reproduced as long as the source is cited with a link to https://www.finder.com/uk/improve-your-credit-score#fraudreport

## About Finder

finder.com is a personal finance website, which helps people compare products so they can make important life choices. Consumers can visit the website to compare investing platforms, banks, credit cards, insurance, cryptocurrency, utilities, mortgages, and so much more.

Best of all, finder.com is completely free to use. We're not a bank or insurer, nor are we owned by one, and we are not a product issuer or a credit provider. We're not affiliated with any one institution or outlet, so it's genuine advice from a team of experts who care about helping you find better.

finder.com launched in the UK in February 2017 and was founded in 2006 by 3 Australians, who still own a majority stake in the business. Finder.com/uk is one of the UK's fastest growing comparison sites, while 10 million people use finder.com each month around the world and over 400,000 rely on the Finder app to manage their money better (source: Similarweb).

Finder commissioned Censuswide to carry out a nationally representative survey of adults aged 18+ between 3 and 7 November, 2023. A total of 2,003 people were questioned throughout Great Britain, with representative quotas for gender, age and region.

For all media enquiries, or for additional comment, contact matt.mckenna@finder.com.

## About the author

George Sweeney is a deputy editor at Finder, specialising in investments and pensions. He has previously written for The Motley Fool UK, Nasdaq, Freetrade, Investing in the Web, MoneyMagpie, Online Mortgage Advisor and Wealth, and is regularly quoted in the national media about investing, pensions and personal finance.