CARD FRAUD

Card fraud 2.0

Card fraud is on the rise despite prevention techniques being more sophisticated than ever. **Chiara Cavaglieri** and **Faye Lipson** investigate why

For a while it appeared the tide had turned on card fraud, but criminals are gaining ground again, despite security checks designed to stop them in their tracks.

Banks say cardholders are being tricked into giving away the keys to their own financial front doors, yet we've previously exposed security flaws that help scammers hijack digital wallets, spend money on cancelled cards and set sneaky subscription traps.

So, what needs to be done? In this special report, we look past the headline figures to examine emerging tactics and how banks are shoring up their defences.

Remote card fraud rife in the UK

Card fraud has affected 14% of UK adults in the past two years, climbing to 20% for 25 to 34-year-olds, according to our recent survey. Many cited tactics such as fake adverts on social media (25%) and search engines (21%), as well as phishing emails (18%), though 25% didn't know how the fraud occurred.

Card-not-present fraud – that is, unauthorised remote purchases made over the internet, phone, or mail order – has long been the main culprit. The UK has seen losses more than double in 20 years and is reported to have the highest rate of remote card theft in Europe. Online security checks, such as one-time passcodes or banking app verification for risky transactions, briefly deterred card fraudsters. But in 2024, total losses increased for the first time since 2018 and the case volume reached record highs.

This increase is a wake-up call after years of security efforts being focused on fighting authorised push payment (APP) scams. 'It marks a shift in tactics by fraudsters who are being frustrated by improved controls in push payments,' says Jonathan Frost of BioCatch, which provides digital fraud prevention technology for the banking sector. 'Fraud is like a balloon – squeeze it and it expands somewhere else.'

Even though the battleground has moved back to cards, the tactics are similar to APP scams: customers are manipulated into sharing sensitive data to scammers impersonating banks and other trusted organisations. 'There is no shame in being socially engineered. If it didn't work, [criminals] wouldn't do it. Everyone is susceptible,' Frost adds.

Our card details can be compromised through no fault of our own. They might be leaked through data breaches, stolen by pickpockets and skimming devices placed at ATMs, or captured by malware-infected browsers, websites and point-of-sale systems.

Reports estimate that 142m stolen card records were posted for sale on the dark web in 2025. A 'Fullz' package is the biggest prize – slang to mean a complete dossier of an individual's sensitive data, including their bank login details, card numbers, email address and any other information an attacker could use to their advantage.

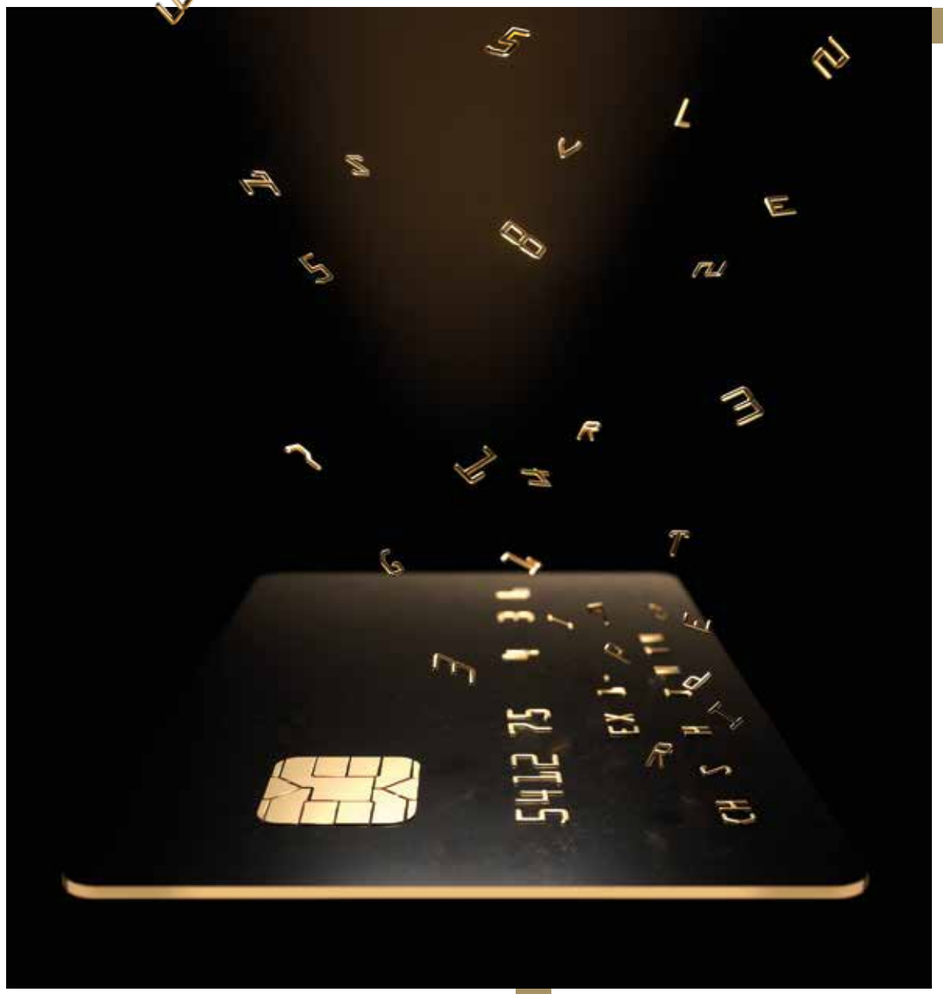


ILLUSTRATION SPOOKY POOKA - DEBUT ART

How card fraudsters cash out

Following the trail of stolen card details is as revealing as it is disturbing. To better understand laundering methods, researchers at University College London conducted a unique operation.

Dr Sharad Agarwal, whose PhD research focused on the lifecycle of SMS scams, partnered with a UK payment processor to monitor stolen credit card details online. These had been intentionally shared with SMS scammers to identify transaction patterns and cash-out methods, safe in the knowledge that these would be blocked because the scammers were given incorrect expiry dates.

'When you try to use card details online, as opposed to a physical machine, a token is sent to the bank to say "somebody's trying to authorise this card"', explains Dr Agarwal. 'When that ping happens, the bank can monitor the transaction data, so we took that raw data and translated it into something more meaningful.'

ONE RAPIDLY GROWING TIER OF CYBERCRIME IS 'FRAUD-AS-A-SERVICE', WHICH ALLOWS AMATEURS TO BUY BESPOKE FRAUD TOOLS, NO DOUBT TURBO-CHARGED BY ARTIFICIAL INTELLIGENCE

He found that the credit card thieves attempted to cash out not only in the UK, but also in Canada, Ireland, the Netherlands and the US. They tried to buy tools and services they could use to conduct further scams, such as VPN services and Sim cards.

Taxi and food delivery apps were also on the hit list, likely because rogue activity flies under the radar due to the high volume of normal transactions.

The rise of industrialised fraud

One rapidly growing tier of cybercrime is 'fraud as a service', which allows amateurs to buy bespoke fraud tools, no doubt turbo-charged by artificial intelligence (AI).

Take the text-scam operation dubbed Lighthouse, selling ready-made templates and backend support on a subscription basis. It's estimated to have reached a million victims across more than 120 countries and was backed by a Chinese cybercrime group, according to a Google lawsuit.

'Ten or 20 years ago you had to be quite technical, but criminal offerings like this mean someone with low levels of experience could get their hands on a dummy website and a phishing kit in about three minutes,' says Garry Lilburn of non-profit intelligence organisation Cyber Defence Alliance.

Scam software can blast out fake text messages by the thousands, using iMessage (Apple) and RCS (Rich Communication Services – Google) as well as traditional SMS. These messaging platforms are fully encrypted, which is great for privacy, but also shields the content from automated interceptors and filters, making it harder to block scams. They also support high-quality images such as corporate logos, giving fake messages a veneer of legitimacy.

A phishing toolkit known as Magic Cat, traced to a Chinese developer and uncovered by computer researchers at Norwegian cybersecurity firm Mnemonic, highlights the industrial scale of modern fraud.

For a weekly licence fee of little more than £100, this software facilitates an entire fraud operation complete with hundreds of copycat website templates (say, Evri and Royal Mail) and is thought to have harvested 884,000 cards globally in just seven months. After successfully infiltrating a Telegram group linked to the operation, Mnemonic found hundreds of Magic Cat scammers discussing strategies and bragging about their lavish purchases.

The scam begins with a fake text, prompting you to click a link to pay a nominal fee – for example, to get a package redelivered. If you click through, you're shown a perfect replica of a legitimate website, save for the web address. As you enter your card details, each character is streamed in real-time to a Magic Cat operator.

When your bank issues a one-time passcode (OTP), you enter this too, assuming you are authorising a low-value payment to a legitimate firm. By the time you close your browser, the scammer has added your card details to a digital wallet on their own device.

Digital pickpocketing

The popularity of mobile wallets has made them an obvious target. Unlike physical cards, Apple Pay and Google Pay have always been exempt from the £100 contactless limit. (The cap for physical cards has now been removed, though many banks have kept it and you can usually set your own limit.) ➤➤

CARD FRAUD

‘I LOST £18,000 TO A DIGITAL WALLET SCAM’

Alexandru, 25, east London
Alexandru was coached by scammers posing as his bank, moving the money from Lloyds to Revolut for ‘security purposes’ before surrendering a single one-time passcode (OTP) that helped the fraudsters clone his card onto their own Apple Pay wallet.

Revolut’s systems did flag the danger, blocking purchases at a cryptocurrency exchange, pawnbroker and luxury store. But Alexandru was still under the scammers’ spell and confirmed his identity to unblock his account.

What followed was a contactless spending spree totalling £16,000 at Selfridges London, £2,200 online, plus a meal at a local restaurant.

This case follows a familiar pattern – a series of high-value transfers, a card registered to a new device and a spate of luxury purchases. Only £1,582 was refunded through chargeback.

Revolut said customers are explicitly told never to share OTPs with anyone else. ‘In this case, our systems identified activity as potentially suspicious and targeted alerts were sent to his Revolut app, which were bypassed.’

We think Revolut should have made more of a clear opportunity to protect a vulnerable customer.

Scammers only need to trick you once to empty your account, as Alexandru discovered to his horror when criminals drained £18,000 in a single day (see left). Some are patient, waiting weeks or even months after stealing your card details, when you and your bank are less likely to sound the alarm and freeze your card. Others are wilier still, calling from a spoofed number from your bank’s ‘fraud department’ to convince you to surrender the OTP sent by your bank, promising this will secure your account or cancel a payment.

Banks have known for years that scammers use social engineering to get hold of OTPs. They also know that SMS is one of the least secure ways to deliver sensitive data, yet most still do this. When we surveyed 14 banks and credit card providers in August last year, only Chase and Monzo told us they don’t use OTPs for digital wallet setups and never have. Capital One takes a conservative approach, barring its cards from being added to digital wallets entirely.

SMS is also susceptible to Sim-swap attacks, where fraudsters convince a mobile provider to transfer your phone number to a Sim card they control so that they can intercept OTPs and potentially take over your banking, email and social media accounts.

Contactless fraud

Other forms of ‘digital pickpocketing’ require a far more technical approach, exploiting near field communication (NFC), the low-power radio signal that powers contactless ‘tap and pay’.

Reassuringly, chip and Pin cards are broadly very safe, benefiting from encryption and unique codes for every transaction. ‘Nobody goes around scanning your data on the Tube,’ says Timur Yunusov, a researcher who specialises in payment systems security. ‘It’s such a faff to target one person and they can only extract the card number and expiry date. What does happen is criminals infecting point-of-sale systems to capture unencrypted card information, especially abroad.’

A more concerning digital sleight of hand is an NFC relay attack, where fraudsters intercept the signal from your card or phone and instantly relay this to another device to complete unauthorised transactions, potentially in another country. They can only do this by distributing malware, often sending SMS and WhatsApp messages that impersonate bank security alerts instructing victims to download fake apps. Some scenarios will require further interaction (to persuade victims to tap their cards on their phones). Others are more passive, as long as the attacker can get close to a victim’s infected phone in a crowded place.

The information gap

While the industry downplays highly sophisticated threats as outliers (one bank told us it had only seen a ‘handful’ of relay fraud cases), cybersecurity researchers warn that NFC scams are surging. Banks work with specialists to proactively detect advanced banking malware threats, but they don’t always have the answers. Take the case of Sahil Gandhi, 34, from Cardiff, who turned to Which? after HSBC refused to refund £4,000 in unauthorised transactions.

He’d been at a gym in central London, leaving his debit and credit cards in a backpack kept inside a Pin-locked locker when two successful debit card transactions were processed in United Arab Emirates dirham (AED), while an attempted credit card transaction (also in AED, equivalent to nearly £3,500) was blocked. His phone hadn’t left his side and his cards were still safely tucked away in his bag.

HSBC initially rejected his claim, insisting the transactions were genuine because the correct Pin had been used. ‘It’s clearly impossible for me to be in Dubai and the UK at the same time,’ Sahil told us. ‘I’m confused as to how this happened. I’ve never been to Dubai. HSBC didn’t believe me and were adamant that I’d written down my Pin. They’re treating me like a fraudster.’ Only after we challenged HSBC on the geographic impossibility of the transaction did it agree to reverse its decision ‘due to the unique nature of the claim.’ It apologised for any stress caused and reimbursed Sahil in full.

We advised Sahil to run a malware scan on his phone and submit a subject access request asking HSBC to share any data related to the incident.

Fraud on cancelled cards

If your bank cancels and replaces your card after fraud, you might breathe a sigh of relief. Unfortunately, our research suggests that the ordeal ➤➤

5 TACTICS TO WATCH OUT FOR

You can no longer assume your card is safe simply because it’s in your physical possession. Criminals have developed bewildering ways to intercept and abuse your card details – sometimes without it leaving your wallet

1 Sim swap
A fraudster tricks your mobile network into transferring your number to a Sim card in their control. They can then intercept one-time passcodes from your bank and gain access to online banking, stealing your card details and setting up mobile wallets.

2 Cloning
Data from your card is stolen from the magnetic strip without your knowledge and placed onto a blank card. This can happen at ATMs where an illegal device has been fitted by criminals; an accompanying hidden camera records your Pin as you input it.

3 Subscription scams
You think you’re making a one-off payment or signing up to a free trial with a legitimate merchant, but in reality it’s a rogue site that has signed you up to a recurring payment for a non-existent, useless or hugely overpriced service.

4 Digital wallet scams
A fraudster adds your stolen card details to a digital wallet (such as Apple Pay, Google Wallet or Samsung Pay) on a device they control. They can then spend in person or at the thousands of online shops integrated with Apple Pay and Google Wallet.

5 SMS scams
A text impersonates a well-known organisation (such as Royal Mail or HMRC) and falsely claims you need to pay a charge or fine. You’re encouraged to click through to a scam website and input your payment and personal details.

How card tech has evolved

A brief history of innovation in card payments and fraud prevention

2001
3D Secure (Verified by Visa and Mastercard SecureCode) is rolled out to prevent card-not-present fraud

2006
Chip and Pin fully replaces signatures to combat magnetic stripe fraud and card theft in the UK

2007
Contactless bank cards are introduced with a limit of £10

2011
Google Wallet and Android Pay arrive in the UK, later followed by Apple Pay, allowing contactless payments via smartphones rather than cards

may not be over. Many of us save our own card details on apps or sites such as Uber, on subscription services such as Netflix, and in mobile wallets such as Apple Pay and Google Wallet. But card details aren't always stored online by their rightful owners. Fraudsters also store victims' stolen card details on accounts and wallets in their control.

When fraud is spotted and a card is cancelled, this isn't always a clean break. In some cases, fraudulent accounts or wallets can be updated automatically with the expiry date and long number of your new card. This tech runs in the background and is provided by the three big card schemes, Visa, Mastercard and American Express (Amex). Each calls it something different, but for ease we'll refer to it as an automatic billing updater (ABU). Card schemes have it switched on by default for banks and issuers, and many major online merchants are opted in.

It's all well and good with a genuine account, when the customer wants that frictionless experience of never having to manually input new card details. It's a lot less desirable with fraudster-controlled accounts, as the ABU risks the fraudster continuing to spend on your replacement card. Banks/issuers normally block ABU updates in the case of fraud, but mistakes can be made.

One banking insider told us fraud teams are sometimes under pressure to hit targets (such as closing a certain number of cases per hour). They also said it isn't always easy for fraud teams to tell whether payments are one-offs or recurring.

Banking body UK Finance also told us of cases in which fraud teams blocked fraudulent payments and ABU updates, but the merchant (or an intermediary payment service provider) circumvented this by reprocessing the payment.

If you haven't heard of ABU, you're not alone; there's very little consumer-facing information provided by the financial industries. Yet fraud continuing on a replacement card appears to be common: of those who have been a victim of card fraud in the past two years, 61% said they had experienced further fraud on their replacement card within three months of receiving it, though not all of these cases will involve ABU.

Too hard to opt out of updates

Last year, Visa and Mastercard both told us cardholders could ask their issuer (the bank or building society who provided their card) to opt them out of ABU so that when a card expires or is cancelled, accounts/wallets would not be updated. Amex (which issues its own credit cards in the UK rather than using banks as middlemen) did not initially say whether such an opt-out was possible on its network.

Opting out of ABU would mean needing to input replacement card details manually, but it could also reduce the risk of fraud continuing on wallets and accounts controlled by scammers. On genuine recurring payments, it could provide friction in a world in which unused or underused subscriptions can roll on for years.

After publishing a piece about this issue in January, we heard from people who said fraud had followed them onto a replacement card. Following Visa and Mastercard's comments, several had tried to opt out of ABU with their bank. None had succeeded; they reported that bank staff seemed confused by the request and/or said it wasn't possible.

We decided to put this to the test. Our team of researchers contacted Amex, Barclays, HSBC, Lloyds, Monzo, Nationwide, NatWest, Santander and Starling and asked to be opted out of ABU on their own card.

In many cases the employee appeared to have no idea what ABU was or what we were asking for. Some incorrectly told us to speak to the card scheme (Visa or Mastercard) instead. Only representatives at Starling and Monzo showed any prior understanding of what ABU was; Starling said it couldn't opt us out, while Monzo said opt-out was only possible via a tick box on screen before a card had been activated. In other words, we would need to order a new card in order to opt out.

What the industry says

Issuers each deal with ABU differently. While in our experiment only Monzo offered us control over ABU, Amex later told us it too lets cardholders opt out by calling the number on the back of their card. Based on our experience, some frontline staff may not be aware of this.

HSBC didn't say whether opt-out was possible. The remaining six issuers confirmed customers can't opt out. All issuers have measures for preventing recurring fraud.

Starling, Monzo and NatWest said that when a card is cancelled due to fraud, they fully opt its replacement out of ABU. This means genuine accounts will need updating.

Amex, Lloyds, Santander and Nationwide said they block payments and/or ABU updates to the particular merchants involved in the fraud (sometimes called 'merchant block').

Mastercard said ABU reduces 'the inconvenience of missed or delayed payments by keeping card details up to date with retailers and service providers. If a card is lost or stolen, these updates are stopped following the cardholder's bank marking the card as closed. Cardholders can opt out via their bank.' It and UK Finance both said fraud linked to ABU is low.

Visa said its service (Visa Account Updater, or VAU) allows 'critical recurring payments to continue without interruptions, even when a card has been updated or replaced. VAU [helps customers by] reducing the chance of declined payments, service interruptions, late fees, and missing critical payments such as life or car insurance.' It added that 'banks are responsible for handling the service for each cardholder, which includes stopping VAU or stopping it for a specific merchant where fraud has been detected.' Visa said it works to keep fraud levels low.

Whichever issuer or card scheme you're with, ongoing vigilance after card fraud is never a bad thing. Nor is questioning your issuer on how it will stop the fraud following you. Unauthorised fraud should almost always be refunded.

Borderless payments

The astronomical rise of internet sales means the door is now wide open to international scammers. Subscription scams have proved to be particularly persistent. Many victims report finding recurring card payments to foreign firms they've never heard of, with no memory of how their details were compromised. We've unmasked many tactics, such as fake QR code stickers linked to phishing websites ➤➤

'MY BANK PERFORMED A "FULL WIPE" TO BREAK THE LINK WITH THE FRAUDSTER'S UBER ACCOUNT'

Faye Lipson

Which? scams experts can be fraud victims too; our research into automatic billing updaters began when I experienced recurring fraud on my own replacement debit card.

Last July I was relaxing on holiday in Cyprus when my bank called out of the blue. Unsure if the call was legitimate, I followed my own frequently dispensed advice by calmly hanging up and calling back using the number on my card.

It was a genuine call by the fraud team to query suspicious attempted transactions with Uber and other retailers.

None of those attempts had been successful. My card was cancelled and replaced, landing on the doormat a few days after I returned to the UK.

Just one month later, payments were successfully taken by Uber for an 'Uber One' subscription using the new long number from my replacement card.

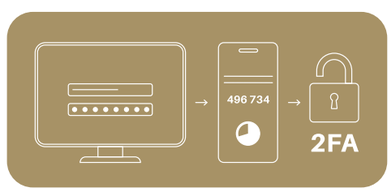
As a fraud expert, I'm extremely careful with my card details and knew I hadn't compromised them myself, especially not so quickly. I asked my bank's fraud team if the fraudster's account on Uber could have automatically received my replacement card details. It confirmed that this can happen.

The card had to be replaced again, and this time my bank performed what it termed a 'full wipe', which broke the link with the fraudster's Uber account and prevented my card being used there again.

One of the fraudulent payments was reimbursed by my bank, and the other was reimbursed by Uber, which apologised for my experience and suspended the user account used to defraud me.

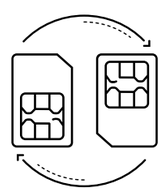
2021
UK contactless limit increases to £30 (2015), then to £45 (2020), and finally to £100 in 2021

2022
Strong customer authentication requires online retailers and payment service providers to implement multi-factor identity checks



2023
Card ID theft losses and cases reach record highs, largely due to criminals hijacking genuine card accounts

2024
Sim-swap attacks surge by 1,055% and card-not-present fraud losses increase for the first time since 2018



2026
£100 contactless limit is removed in March, but many banks are keeping it in place for now

‘MY REPLACEMENT CARD WAS REPEATEDLY COMPROMISED’

Martyn Evans, Cumbria
In December, immediately after shopping online, Martyn was tricked by a fake Evri webpage that said he needed to pay a small fee. He entered details of his Pluxee prepaid debit card, before quickly realising he’d been scammed and contacting Pluxee to cancel the card.

He received a replacement card from Pluxee and, thinking he was now safe from the fraud, uploaded £400 to it.

In January, Martyn checked his statement and was horrified to discover that more than £200 had been spent using his old card number almost 300 miles away. Using Apple Pay, a fraudster had made three payments, including £225 at a designer handbag shop.

So Martyn contacted Pluxee again. The firm said it had correctly identified and blocked the fraudulent wallet the first time Martyn called. But in rare cases, fraud can continue if the fraudster disconnects the device from the network because mobile wallets will allow a limited number of ‘offline’ transactions before ceasing completely.

Pluxee said: ‘This incident arose from a third-party scam, of which the cardholder was an unwitting victim. When they reported suspicious transactions in December, we acted swiftly to secure the account. Our fraud controls operated as intended, and there was no compromise of Pluxee’s systems.’

The company stated that it ‘takes the protection of its cardholders extremely seriously and has robust controls in place to detect and respond to fraudulent activity.’

Pluxee added: ‘When further queries were raised in January, the matter was promptly escalated and the full value of the disputed funds was reimbursed within 48 hours.’

PHOTOGRAPHY: GEORGE CARRICK - UNP

at car parks, copycat apps advertised on search engines and bogus shopping deals spread via social media.

Refunds are by no means guaranteed either, because banks and other payment firms treat these as authorised transactions, failing to acknowledge that the ‘authority’ was only gained through misleading ads and other underhand tactics.

It’s clearly a struggle to keep a lid on rogue foreign businesses – in 2024, a staggering 75% of online card-not-present fraud occurred at a merchant acquired outside the UK. Scammers are sly too, obtaining a whole series of merchant accounts across different markets, switching between them to avoid hitting the thresholds that might have them (or their acquirer) banned.

The prevention balancing act

The banking industry has a long history of playing cat and mouse with fraudsters. After the launch of chip and Pin in 2006 to combat card theft and cloning, criminals quickly turned to using stolen card details remotely, buoyed by the surge in online shopping. Strong customer authentication ironed out many flaws and standardised security, although the Home Office recently announced plans to repeal these technical standards to ‘support the adoption of new technologies’ and enable firms to apply ‘proportionate, risk-based measures for low-risk transactions’.

Balancing security and modern demands for speed and convenience requires a deft hand and fraud teams are under relentless pressure to match their defences to criminals’ ever-evolving tactics.

DATA ANALYSIS IS THE KEY TO FIGHTING FRAUD IN THE DIGITAL AGE

Data analysis is the key to fighting fraud in the digital age. Banks can measure the likeliness of transactions being safe by using machine learning models to spot suspicious activity the moment it happens. ‘One of our successes has been monitoring test transactions,’ says Jim Winters, Nationwide’s director of economic crime. ‘Scammers tend to test a bunch of card details all at the same time. So we might see a raft of them coming in, which gives the game away.’

Anomalous behaviour is another way the industry can detect fraud, using in-house tools and intelligence, or working with companies such as BioCatch, Cleafy, LexisNexis and ThreatFabric. Banks should be able to build a highly detailed digital profile of your typical behaviours, recording how you type, how you touch your screen and which wi-fi network or browser you prefer to use. It should be looking for signs that you’ve been hacked, as well as evidence that you might be being coached by scammers, eg by detecting that you are on a call at the time of a transaction.

Winning this arms race will also require collaboration across the banking industry and other sectors. Cybercriminals don’t just stay in one lane, says Mike Nathan of LexisNexis Risk Solutions. ‘They are channel agnostic – it’s the whole ecosystem that they’re attacking.’

If we’re really going to tackle card fraud and other threats at scale, simply warning customers not to share passcodes isn’t going to cut it.

How to avoid card fraud

- Turn on two-factor authentication (2FA) for all of your online accounts, ideally using passkeys or authenticator apps (supported by Apple, Google, Microsoft and Samsung).
- Use bank fraud tools such as instant card freezing and other controls – some bank apps let you turn off remote purchases and contactless payments if you’re worried your card details have been stolen or added to a digital wallet.
- Scrutinise website URLs carefully and avoid clicking on links sent in unsolicited messages, shared on social media, or advertised on search engines.
- Check the domain age before you enter your card details online using lookup tools such as Who.is – be suspicious of newly created websites.
- Try virtual debit cards offered by Chase, Monzo, NatWest Group, Revolut and Starling, so that you don’t share real card details with unfamiliar (and therefore risky) websites.
- Secure your mobile account by asking your network to add a secondary Pin or password which must be provided before it issues a Sim swap or PAC code.
- To protect your phone, add a unique Pin to your Sim, disable preview notifications which could be viewed by a thief, and use Google’s Find My Device or Apple’s Find My iPhone.

Note: The figures in this article are based on a survey of 2,079 members of the public and are representative of the UK population aged 18+. Data collection was conducted online in March 2026.

NEXT STEPS

Always report suspected fraud on your card or account to your bank immediately. Call 159 (run by Stop Scams UK) to reach its fraud team quickly. If you’re unsatisfied with your bank’s response, the Financial Ombudsman Service may be able to help: **financial-ombudsman.org.uk**

ONLINE
- Sign up to our scam alerts: *which.co.uk/scam-alerts*
- More on digital wallet fraud: *which.co.uk/walletfraud*

Contactless fraud – how big is the risk?

Some risks of card fraud are hugely exaggerated in the public imagination, while others are underplayed. Many people worry about their physical card’s chip being maliciously scanned from within their bag, in crowded areas such as busy shops and airports, by a criminal armed with a card scanner. There’s a roaring trade online in RFID wallets that claim to block such attempts.

In reality, the risk of this happening is vanishingly small. UK Finance confirmed in February 2026 that there have been no recorded cases of criminals walking into a public place with a contactless card reader and initiating unauthorised transactions. Those wallets aren’t harmful, but you really don’t need one.

In a similar vein, our survey found 24% of people incorrectly believed that in densely populated areas such as flats, a microwave could be used to scan neighbours’ card details. A further 27% were unsure if it was true. This is an outright myth. In reality, the greatest risk comes online: either from being tricked into divulging your own card details, or from having them exposed in a large data breach (for example, a major retailer that stores huge numbers of customer card details).

That’s why being very cautious with your data – who you give it to, and where you save it – is far more effective than wrapping your card in foil.