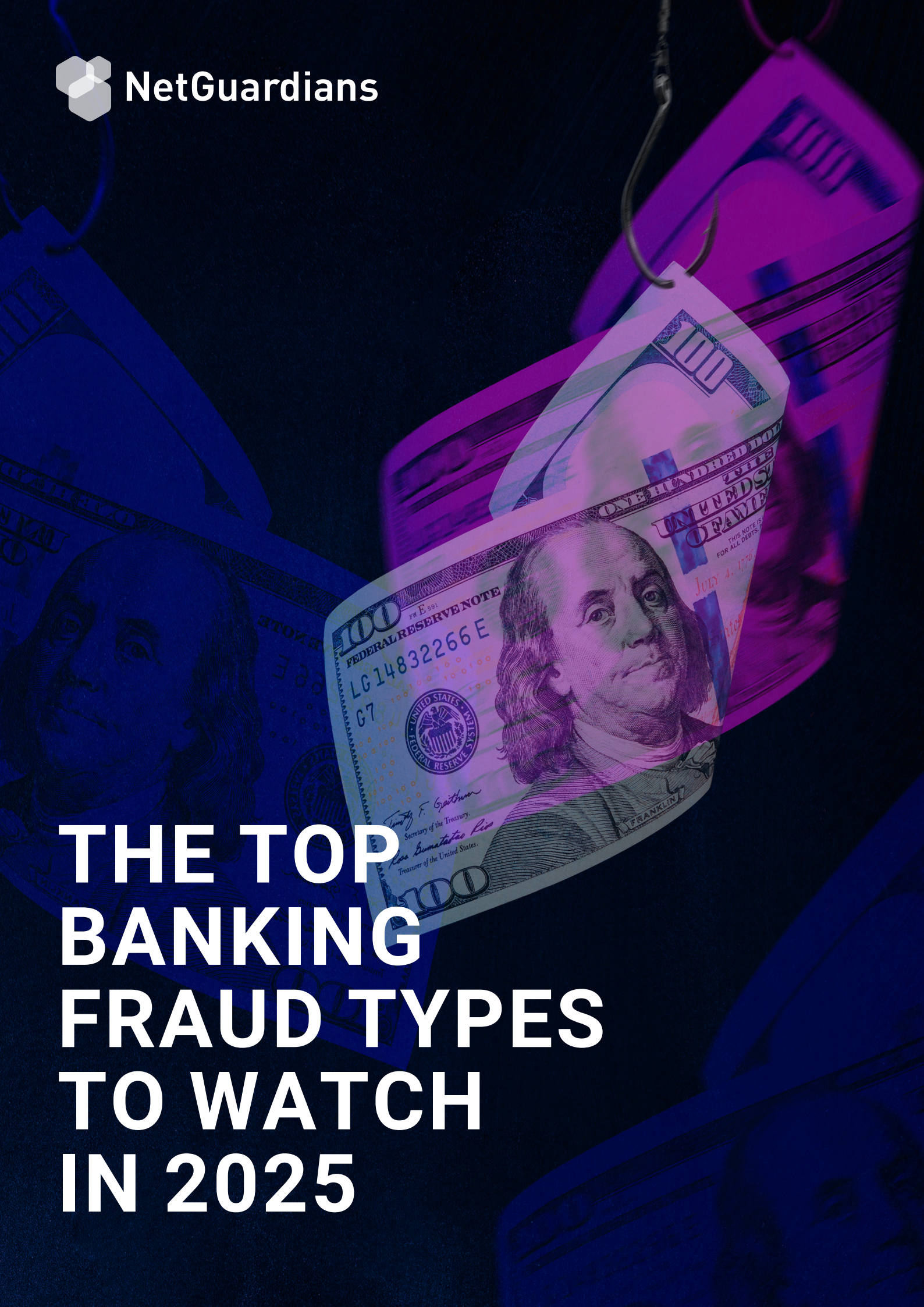
NetGuardians



THE TOP BANKING FRAUD TYPES TO WATCH IN 2025

Introduction

As we predicted in our previous report, fraud surged in 2024 and is showing no signs of slowing down in 2025.

$1.03 trillion
worldwide losses from fraud in 2024

The latest global fraud stats are alarming. Not only is fraud continuing to increase, but it is becoming more sophisticated and complex.

According to the 2024 Global State of Scams Report from non-profit GASA (the Global Anti-Scam Alliance), worldwide losses from fraud increased to $1.03 trillion last year. The report surveyed 58,329 people across 42 countries. It found that almost half the world's population encountered criminal scamming attempts at least once a week, and a third of those living in Hong Kong and a quarter of those living in South Korea were targeted every day. The study shows losses per victim in the United States reached an average of $3,520, followed by $3,067 in Denmark and $2,980 in Switzerland. Losses equaled 3.6 percent of Gross Domestic Product in Kenya and 3.4 percent in Thailand and South Africa.

If you've been defrauded once, it does not make you less likely to be defrauded again. According to the UK's National Fraud Helpline, a third of victims have been defrauded more than once, with criminals selling their data on to other scammers.

The human impact of scams

Only 4% of victims fully reimbursed

Victims often lose their life savings and fraudsters go unpunished. Reporting is hindered by complexity, a sense of futility and embarrassment. Admitting to being deceived – especially in scams like romance fraud where emotions are exploited – is a daunting challenge for many.

But the human toll of scams is not unique to victims. Criminal gangs are the equivalent of modern slavery bosses, trafficking people across borders, holding them against their will and forcing them to initiate scams from call centers operating on an industrial scale.

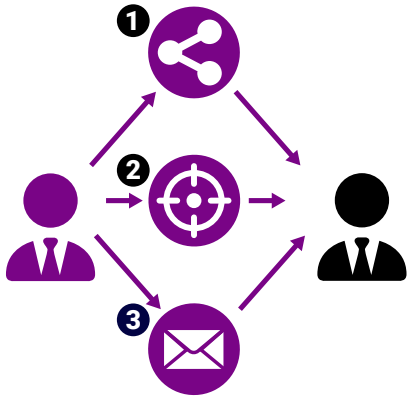
Yet despite the enormous human cost, in the GASA's 2024 report, just 28 percent of respondents reported scams or attempts at scams to the authorities. Some sources suggest significantly lower numbers – the National Crime Agency in the UK states that just 13 percent of frauds are being reported. Globally, only 4 percent of victims were able to recover all the money lost.

America's Federal Trade Commission believes adults aged 60 and older are more vulnerable to fraudsters than younger peers, losing an estimated $61.5 billion in 2023. Often, they are gulled by fraudulent investment schemes, fake computer support offers or worthless gift vouchers.

However, many younger people are also fooled by scammers. Artificial intelligence (AI) is being used, for example, to create fraudulent documents that closely resemble legitimate letters or invoices. But the links they contain may connect to fake corporate websites or contain QR payment codes that transfer funds to criminal accounts.

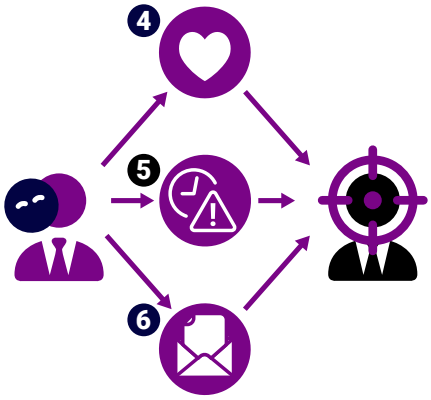
The scam attack chain

A TARGET AND PREPARATON



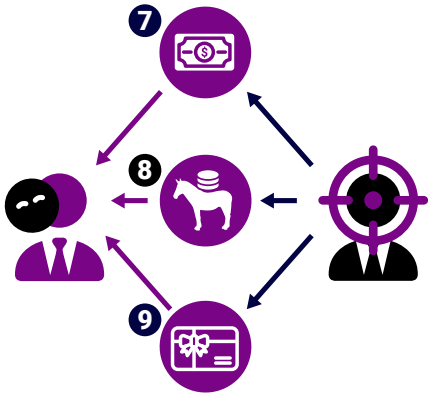
1. Reconnaissance: Open-source intelligence (OSINT) tools used to research personal information
2. Potential target identified
3. Impersonation preparation: Fake identities, emails or websites created to win trust

B SCAM EXECUTION



4. Manipulate or psychologically trick target with deceptive offers (fake job offers, lottery wins or investment opportunities)
5. Add a sense of urgency or build trust and rapport
6. Request money transfers or sensitive information

C MONEY TRANSFER



7. Convince target to wire money to scammer-controlled account
8. Or to money mules used to obscure scammer's identity and location
9. Cryptocurrency payments, gift cards or prepaid cards often requested as they are harder to trace

How the scammers get you

All fraud originates with 'social engineering' whereby fraudsters manipulate or trick customers, employees or third parties and exploit human error to gain access to private information, sensitive data, restricted systems or assets.

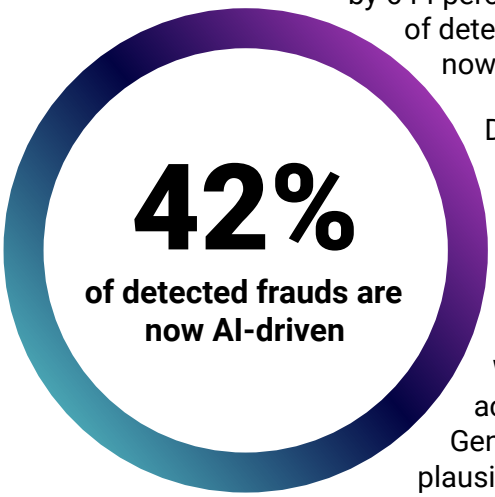
The most frequently reported online scams, according to the FBI's April 2024 Internet Crime Report, involved "phishing schemes, which use unsolicited emails, text messages and telephone calls purportedly from a legitimate company to request personal, financial and/or login credentials."

Phishing is scalable, low cost, difficult to trace and accessible to attackers of varying skill levels. Using data from previous phishing attempts or research on social media enables emails, calls or texts ('smishing') to be personalized and aimed at specific people ('spear phishing'). While the majority of these attacks focus on individual consumers, fraudsters are also stealing significant sums from companies by targeting executives and employees through 'CEO fraud' and business email compromise (BEC), payment service providers (PSPs) and payment infrastructures.

Increasingly, fraudsters are using a mix of technology and social engineering to introduce malware into an individual's or company's digital ecosystem to steal funds. Spear phishing messages are also often facilitated by crime- or fraud-as-a-service schemes and troves of stolen data offered for sale on the dark web. Within this fraud landscape, AI is set to prove a game-changer.

The dark side of AI

Looking ahead, the big difference between 2024 and 2025 will be the far wider application of AI by fraudsters. We know, for example, that they are sharing how to use AI to harvest information to use against targets and set up scams over messaging platforms such as Telegram. Indeed, research by Point Predictive found conversations over Telegram that included the terms AI and deepfakes increased by 644 percent last year. Research also revealed that 42 percent of detected frauds in the payments and financial sector are now AI-driven.



Drilling further down into fraud types and success rates remains difficult as AI technologies are still too new. Nevertheless, the threat is serious enough to have caused the FBI in early December 2024 to warn that criminals are exploiting AI-generated text and imagery including photos and videos, as well as voice cloning to reach their targets.

Without doubt, AI will increasingly be incorporated across many fraud types in the coming months and years. Generative AI will help to make spam communications more plausible by eliminating typos, poor grammar and inappropriate language, as well as facilitating voice cloning, deepfakes, fake LinkedIn personas and fake websites, making scams harder to spot.

We also expect fraudsters to up their use of AI to analyze a potential target's online and social media presence to help them personalize phishing attacks to increase their credibility. There's also evidence to suggest that voice-enabled AI Agents – fully automated bots – are being used on a huge scale to autonomously steal social media or email credentials, convince targets to share sensitive information, access bank accounts and transfer money.

The fraud trends report

Scam definition: The use of deception or manipulation intended to achieve financial gain

Creative, innovative, persistent, determined, ruthless, fast, cutting-edge. Fraudsters with their eyes on your money are all of these as they try to stay one step ahead. But knowing how they operate and the techniques they use will help stop them.

Their techniques fall into two categories: authorized push payments (scams), when the target is duped into making a payment; and unauthorized payments (fraud), when the criminal has obtained enough information to initiate and complete a transaction without the bank account owner being involved.

Here we look at some of the scam and fraud types and techniques – new and well established – that we think will dominate 2025. As most of them are scams, our classification process has followed the Federal Reserve's ScamClassifier model.

Launched in June 2024, the model enables consistent, detailed classification, reporting, analysis and identification of scams, attempted scams and related trends. The aim is to gather consistent and quality data to be better able to stop the fraudsters.

For frauds, we use the FraudClassifier.

Predicted top 10 scams and frauds in 2025

		Authorized	Unauthorized
1.	CEO fraud/impersonation scam	●	○
2.	Bank employee or police impersonation	●	○
3.	Romance scam	●	○
4.	Investment scam	●	○
5.	Online purchase scam	●	○
6.	Phishing-enabled account takeover	●	●
7.	QR-code fraud	●	○
8.	Invoice scam	●	○
9.	Technical support scam	●	●
10.	Advance fee scam	●	○

The scams

Authorized push payments*

Unauthorized payments*

As per the Federal Reserve's ScamClassifier

CEO fraud / Impersonation scam

Business Impostor

While people have always impersonated others to get what they want, the increasing application of AI is making it easier for scammers to be convincing. Typically, they impersonate senior management or a close friend or relative in emails, voice notes or text messages to convince the target to initiate a cash transfer to a fake account – an authorized push payment. They use Gen AI to recreate the written style, voice and/or image of the person being impersonated, making the scam far harder to spot.

This scam is growing worldwide. Australia saw a 37 percent jump with 302,000 reported incidents between 2022 and 2023. Meanwhile in Spain, police last year arrested a gang that had used the "Hi mum scam," pretending to be a child who needs money – often to replace a lost phone – to con at least €410,000 from hundreds of victims.

PREVENTION

- Install and keep up-to-date firewalls to stop scammers hacking into email accounts to gain information
- Check images and videos for signs of manipulation such as poor focus or lack of movement
- Train staff to be vigilant
- Adopt robust protocols for verifying new-destination bank accounts
- Share a safe word with family and friends to prove identity
- Report any suspicious activity
- Adoption by banks of smarter, AI-enabled software that can detect anomalies within the account and the transaction and flag unsafe payments for further investigation

Case study

SCENARIO

A fraudster compromised the email account of an employee responsible for authorizing payments. He then impersonated the CEO in emails using a spoofed email address and convinced the employee to transfer CHF 58,930 to a UK IBAN via e-banking.

SOLUTION

NetGuardians software spotted the unusual destination and raised an alert. The bank contacted the company and the employee confirmed the transaction. Drawing on details of the alert, the bank convinced the employee to double-check. A company director confirmed the payment was fraudulent and the bank blocked the payment, preventing the funds from being transferred to the fraudsters' account.

2 Bank employee or police impersonation

Bank/Government Impostor

One of the most established fraud types, in which scammers pretend to be bank employees or law enforcement officers to trick targets into revealing sensitive financial information. They often contact targets through phone calls, emails or text messages, claiming there's an urgent issue such as a security breach or an ongoing investigation. Leveraging a sense of urgency, they convince targets to share account details, transfer money or download harmful software. According to Interpol[16], this type of fraud is particularly prevalent across the Americas and Asia.

PREVENTION

- Avoid sharing personal information with unsolicited contacts
- Always verify calls through official sources
- Report any suspicious activity
- Adoption by banks of smarter, AI-enabled software that can detect anomalies within the account and the transaction and flag unsafe payments for further investigation

In a variation of the bank employee impersonation scam, the scammer contacts the target claiming to be from the bank's security team and warns of a supposed threat to their account. They insist the target's funds need to be moved to a more secure location, often suggesting a different bank or account. To build trust, the scammer may even provide fake confirmation messages or details of supposed security breaches. The target is then manipulated into transferring money, often through multiple smaller transfers, which are harder to trace. By the time the target realizes it's a scam, the money is gone. Again, this fraud is widely seen in Asia, according to the international law enforcement organization.

Awareness campaigns and bank protocols helped cut the number of impersonation frauds in the UK in 2023. They fell by 37 percent, with the total defrauded down 28 percent. Elsewhere in the world, however, this fraud is still on the rise. For example, complaints to the Australian Financial Complaints Authority about bank impersonation scams hit 9,000 in 2023, nearly double the previous year.

Case study

SCENARIO

A customer was called by a fake police officer and then by a fake bank employee. The two fraudsters convinced the customer to transfer CHF 47,000 to another bank in Switzerland on the grounds that their bank account had been compromised.

SOLUTION

NetGuardians software blocked the transaction due to the unusual amount. Using insights from NetGuardians' Community Intelligence model, which shares insights on suspicious beneficiaries (for more information see Community Scoring and Intelligence), the software flagged the recipient as previously linked to suspicious payments, strengthening the alert.

3 Romance scam

Romance Impostor

According to Interpol, romance scams started in Asia in 2019 and expanded during the Covid-19 pandemic. Today, they are a global problem, with criminal gangs from every continent faking love to steal your money on an industrial scale. South-East Asia remains a major hot spot, with gangs setting up call centers to target Europe in particular, according to the international law enforcement organization.

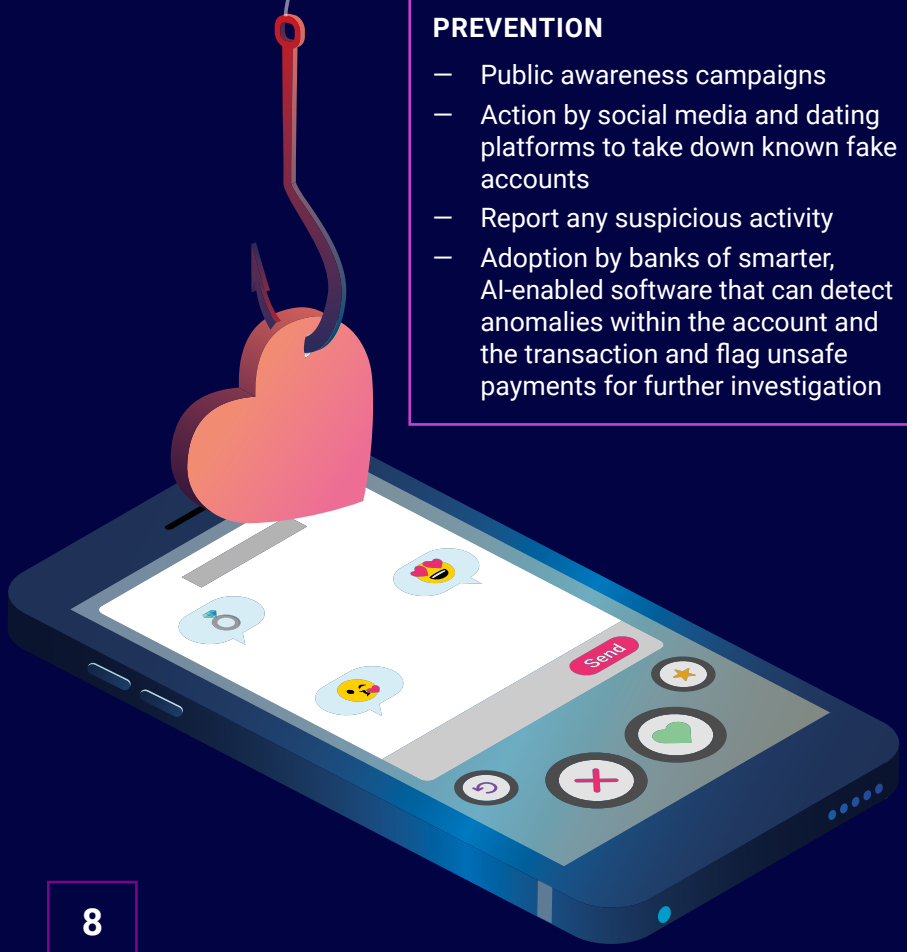
Historically, the target was approached via text message, email, social media or dating platform and drawn into a long-distance relationship. More recently, the scammers are using AI-powered image-generation software to make video calls to targets using deepfake video feeds. The software allows fraudsters to animate a still photograph so they can speak to the target on a video call, using the appearance of the person in the photo. The generative AI software animates the deepfake image allowing the target to see the deepfake avatar speaking the scammer's words and reproducing facial expressions in real time.

25%
of dating app users affected by romance scams

This is exactly the playbook of scammers who convinced a wealthy French woman to hand over €830,000. They had spent months convincing her she was in a long-distance relationship with actor Brad Pitt, using AI to manipulate images and videos in a scam that went on for more than 18 months.

Whether AI is used or not, the scam unfolds in the same way. Once the target is drawn in, the fraudster typically requests money transfers – authorized push payments – to allow them to meet or clear debts. Even after attempted romance frauds are flagged by their bank, targets often insist on authorizing the payments. This demonstrates the power of romance scams to dupe targets, who want to believe they have found love. Banks need to be able to show that the payment is going somewhere other than where the target thinks.

According to cybersecurity specialist Norton, online romance scams jumped 72 percent last year, affecting more than one in four dating app users, with nearly one in three being 'catfished' by fake personas.



PREVENTION

- Public awareness campaigns
- Action by social media and dating platforms to take down known fake accounts
- Report any suspicious activity
- Adoption by banks of smarter, AI-enabled software that can detect anomalies within the account and the transaction and flag unsafe payments for further investigation

Case study

SCENARIO

The target met the fraudster online and believed they were in a genuine romantic relationship. The fraudster claimed to be in financial difficulties and asked the client for help, requesting transactions up to €4,000.

SOLUTION

NetGuardians software stopped the transactions, spotting unusual variables, including the beneficiary bank account, destination country, amount and currency. The data supplied by NetGuardians helped the bank convince the target of the fraud and payments were blocked.

Investment scam

Investment

Get-rich-quick, or investment scams, are possibly one of the oldest in the criminal playbook, but today the internet has boosted the reach of fraudsters to make them a far bigger problem.

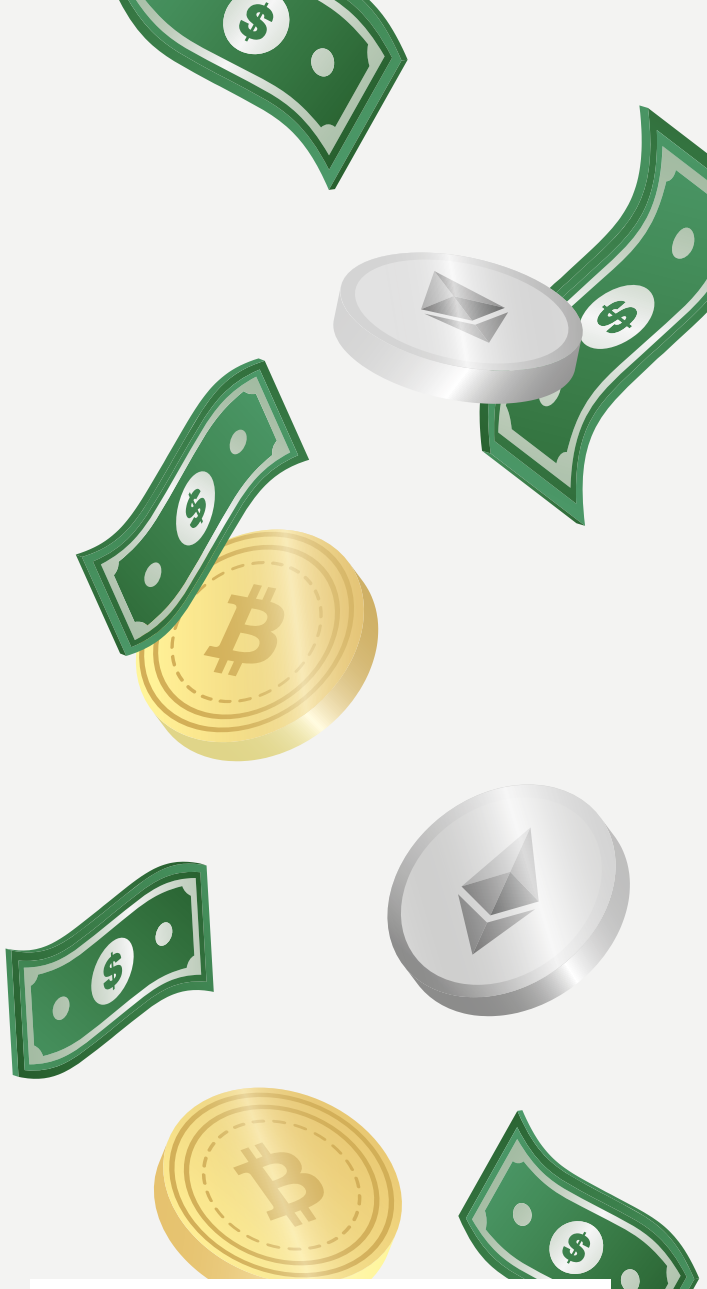
Online investment forums on cryptocurrencies, growth trends and special opportunities, as well as the ability to send emails and make phone calls using addresses and numbers stolen in data breaches, give fraudsters almost unlimited reach. AI analytics programs allow them to scrape the internet for personal information that helps target potential targets with highly personalized approaches, while Gen AI gives them the tools to create convincing false personas, websites, LinkedIn profiles and more to make it harder to spot fake from reality. These scams are about getting targets to "invest" in spurious schemes, with the target authorizing the payment transfers.

Typically, an investment scam target is groomed slowly, and the technique is combined with a romance scam. Payments often increase over time. Fraud followers are expecting 2025 to see a big increase in this, particularly in the cryptocurrency area.

Already viewed by Interpol as one of the more prevalent scams in Europe, its return on effort for the scammers is high. According to UK bank Barclays, investment scams last year netted the highest average sum per scam – £15,564 – but represented just 4 percent of all such activity. This makes it highly attractive to scammers and therefore likely to become more common.

PREVENTION

- Beware of unsolicited contact
- Resist pressure to invest without time to check out the proposition
- If it's too good to be true, it's probably a scam
- Report any suspicious activity
- Adoption by banks of smarter, AI-enabled software that can detect anomalies within the account and the transaction and flag unsafe payments for further investigation



Case study

SCENARIO

A target fell for a fraudster offering a cryptocurrency investment opportunity that promised significant returns in exchange for advance payments. He made three substantial payments.

SOLUTION

NetGuardians software spotted the unusual amount being transferred. When the target was contacted, he disregarded the bank's warning that he had fallen for an investment scam and made further payments. Ultimately, the suspicious activity, coupled with insights about the beneficiary gained from NetGuardians community and intelligence model, foiled the fraudsters.

Online purchase scam

Merchandise

This scam involves fake online stores that allow scammers to do two things: obtain customer bank information they can use for subsequent unauthorized purchases; and sell products and services that never arrive.

Increasingly, the scammers are using Gen AI to create more authentic-looking websites, often closely impersonating real businesses, and using 'SEO poisoning' – where SEO rankings are manipulated to make the website appear higher up in search engine results – to attract traffic.

One of the most frequent types of scam, online purchase scams were found by research group Statista to have accounted for 41 percent of all such activity worldwide in 2023. This is not surprising when you look at how these scams are operated.

According to research by cybersecurity specialist SR Labs, one Chinese operator of bogus sites had industrialized its operations on a global scale. It had scammed more than 850,000 victims across Europe and the US out of more than $50 million since setting up shop in 2021. SR Labs found some 75,000 bogus sites linked to the group, with 22,500 active sites as of April 2024.

Case study

SCENARIO

A target found a fake advertisement for a fake website selling electric bikes and paid €1,800 to purchase goods

SOLUTION

NetGuardians software spotted the unusual beneficiary account and amount and raised an alert. The bank reviewed the payment and called the target, alerted them to the high likelihood of a scam, and the payment was stopped.

PREVENTION

- Check the URL matches the known company
- Be cautious when clicking on sponsored links
- If a deal appears too good to be true, it's probably a scam
- Report any suspicious activity
- Adoption by banks of smarter, AI-enabled software that can detect anomalies within the account and the transaction to flag unsafe payments for further investigation

6 Phishing-enabled account takeover

Compromised Credentials

Once the criminals have a target's bank and card details, they can use them to go on a spending spree – unauthorized payments. This is classified as a fraud rather than a scam by the Federal Reserve and is included in its FraudClassifier.

Fraudsters get the details through phishing emails, often purporting to be from banks, companies, delivery agents, tax authorities, health services and many other sources (see Online Purchase Scam #5). The emails contain links that, once clicked on, automatically download and install a piece of malware on the target's device. This gathers personal information needed for an account takeover. We expect Gen AI to become an important enabler of this kind of fraud in 2025, while AI-driven bots will allow scammers to make many purchases over a very short time.

In the US, unauthorized card purchases exceeded $5 billion last year.

PREVENTION

- Public awareness campaigns to avoid clicking on suspicious links
- Report any suspicious activity
- Adoption by banks of smarter, AI-enabled software that can detect anomalies within the account and the transaction and flag unsafe payments for further investigation

Case study

SCENARIO

Scammers received a target's phone number from a marketplace platform and managed to gain access to his e-banking credentials. They initiated two unauthorized payments of CHF 14,500 and CHF 9,650. Both payments were directed to two different Swiss IBANs.

SOLUTION

NetGuardians software spotted anomalies within the transactions, including the value, beneficiary accounts, time spent on the application to perform transactions and the sequence of the scammer's actions. It raised alerts by the target's bank that ultimately led to the payments being stopped.

7 QR-code fraud

Business Impostor

A newer fraud type widely known as 'quishing,' scammers use fake QR codes to trick people into making payments or revealing sensitive information. The most common form of quishing is fake QR codes for payment fraud.

A scammer places a fake QR code on a product, bill or in a public space, making it look like it's from a legitimate business or payment service. When someone scans the code, they are directed to a fake website or payment page controlled by the fraudster. The target then enters their payment details or makes a transfer to the scammer's account – an authorized payment.

This type of fraud often occurs in places where people are paying for services or goods, such as restaurants, car parks, shops or even online marketplaces. In 2024, Belgium saw several quishing attacks using rogue QR codes, including on cash machines in Bruges and on parking meters in Brussels. These are typical of quishing scams worldwide.

PREVENTION

- Check whether the code has been covered with a false QR code sticker
- Always double-check the URL of any link from a QR code
- Avoid downloads
- Report any suspicious activity
- Adoption by banks of smarter, AI-enabled software that can detect anomalies within the account and the transaction, and flag unsafe payments for further investigation

Case study

SCENARIO

A target received a letter appearing to be from a known and recurring supplier. To make the payment, the target scanned the QR code and proceeded to pay €1,845.

SOLUTION

NetGuardians software blocked the transaction due to the unusual amount. Using insights from NetGuardians Community Intelligence model, which shares insights on suspicious beneficiaries (for more information see Community Scoring and Intelligence), the software flagged the recipient as previously linked to suspicious payments, strengthening the alert. The bank rejected payment.

1/3

of UK businesses were victims of *invoice* scams in 2024

8. Invoice scam

Business Impostor

This scam involves a fraudster sending a fake invoice for payment which is then authorized by the target. The invoice can be from a fake company for something never delivered or from a spoofed company – one created to look exactly like a real company, but with fake bank details. Gen AI is increasingly being incorporated into invoice scams, helping the fraudsters appear genuine.

Last year, nearly one-third of UK businesses fell victim to this type of fraud and more than three-fifths were unable to stop the transactions before they were finalized.

PREVENTION

- Check the email address that sent the invoice matches the company email exactly
- Adopt robust new supplier protocols
- Report any suspicious activity
- Adoption by banks of smarter, AI-enabled software that can detect anomalies within the account and the transaction, and flag unsafe payments for further investigation

Case study

SCENARIO

An employee in a company in the auto industry in Germany received a fake €251 invoice for trademark registration services in Spain. As the amount was typical for such services, the employee approved payment, even though the company had never sought such services beyond Germany.

SOLUTION

NetGuardians software detected and blocked the fraud due to the unusual amount, destination country and bank.

Technical support scam

Business Impostor

Fraudsters exploit the tech support scam by posing as help-desk agents for tech companies. Their goal is either to install malware that steals banking details or to extract payments by claiming to fix non-existent problems. Their tactics typically include instilling fear at the prospect of catastrophic damage unless their warnings are acted on and using jargon and technical terms to impress and confuse the target into complying. They often target older people.

Despite many warnings from tech companies and law enforcement, these scams continue to succeed. In 2023, they netted the fraudsters nearly $1 billion in the US alone, while NetGuardians' own research indicates a spike in the fourth quarter of 2024.

PREVENTION

- Awareness campaigns about how bone fide companies contact customers
- Report any suspicious activity
- Adoption by banks of smarter, AI-enabled software that can detect anomalies within the account and the transaction and flag unsafe payments for further investigation

Case study

SCENARIO

A target had been browsing the web when a message popped up warning that the computer had been infected and gave a local number to call. He called the number and the scammer asked him to install a screen-sharing tool and performed some tests. They then asked him for an e-banking payment. This gave enough e-banking credentials to the scammer to initiate many payments, including $7,500 to an illicit account in Lithuania.

SOLUTION

NetGuardians software spotted the first transaction was genuine, but that the second was suspicious. Not only was the destination account new, but our community intelligence model recognized that it was linked to other suspicious activity. The transaction was successfully blocked before any money left the account.

$1 billion

lost to technical support scams in the US in 2023

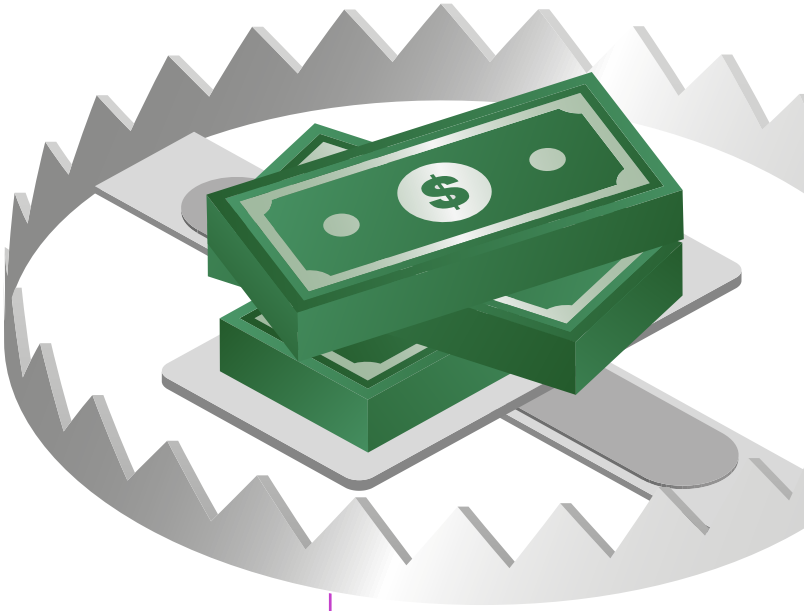
10 Advance fee scam

Business Impostor

These scams take in several scenarios, from unlocking a fake inheritance to paying for a parcel sent with insufficient postage. The scammers' goal is either to gather personal information they can use to hack bank accounts so they can make unauthorized payments or to trigger a direct payment into a fake account – authorized payments. These scammers, like e-commerce scammers, operate on an industrial scale. One Chinese smishing gang was found to be sending between 50,000 and 100,000 texts a day.

Typically, the scammer will contact a target by text or email claiming to be a lawyer or delivery service with something that needs a payment to be released. The communication will include a link to make payment.

In the US, the national postal service regularly warns the public about this type of scam due to its prevalence, with the latest warning coming just before Christmas – peak posting season. According to Interpol, these scams are widely seen in the Americas and Africa.



PREVENTION

- Beware of unsolicited contact
- Check the URL of any link exactly matches the company it claims to represent
- Decline to pay up-front fees
- Report any suspicious activity
- Adoption by banks of smarter, AI-enabled software that can detect anomalies within the account and the transaction and flag unsafe payments for further investigation

Case study

SCENARIO

A scammer got in touch with the target about an inheritance that needed a €4,500 payment for it to be released. The target initiated the payment.

SOLUTION

NetGuardians software blocked the transaction due to the unusual amount, beneficiary and country. In addition, the community intelligence model revealed the beneficiary was already known and linked to suspicious payments, adding weight to the alert.

How scammers clean their money

Scammers often launder money using methods like cryptocurrency, gift cards or prepaid cards, which provide anonymity and are harder to trace. While direct bank transfers can leave a trail, stricter anti-money-laundering regulations have made moving stolen funds offshore more difficult, leading scammers to rely more on money mules. AML transaction monitoring, like NetGuardians' solution, empowers banks to identify a greater proportion of money-laundering transactions, providing up to 10 times fewer false alerts than traditional rule-engine approaches, thus saving time, improving efficiency and reducing risk.

Domestic money mules are victims of fraudsters and are often recruited via social media with offers of cash payments. They unwittingly or knowingly move stolen money through their accounts, disguising its origins. A 2024 study by Lloyds Bank found that young people were often targeted, with 58 percent aged between 19 and 40.

How AI can help fight fraud

While AI is being used by the criminals, it can also be used in the fight against fraud. Generative AI can usually tell you if a document was created by artificial intelligence – unless the AI was asked to create a document whose AI origins were undetectable. Crime-busters have always to think one step ahead.

AI is also superb at identifying behavior that doesn't fit with previous patterns and this extends to money mules. AI-powered fraud-prevention software can now spot many of these transfers in real time and alert banks to freeze the transactions.

Education and mitigation

Fighting scams and other financial crimes must be a collective effort. It takes ongoing consumer education, including for teenagers and the elderly who, for different reasons, are less alert to the antics of online scammers.

In the US, the FBI has worked with local broadcasters to launch its 'Take A Beat' campaign against online fraud, backed by a website and fraud hotline. And the American Bankers Association renewed its annual anti-phishing campaign under the slogan: "Banks Never Ask That!"

Meanwhile, urged on by America's Cyber Defense Agency, companies are becoming increasingly aware of the need to train employees not merely to spot online fraud, but also to avoid sharing on social media or other platforms information that could help scammers compile fake employee profiles and other forms of social engineering.

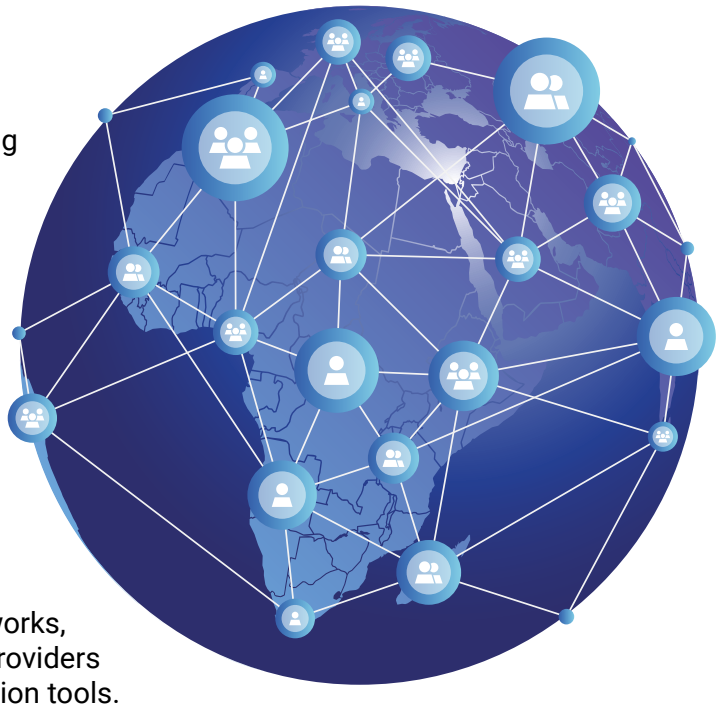
Regulation

Regulators are creating rules for financial institutions to do more to combat fraud. For example, in the UK, authorized push payment (APP) scams, where the fraudster persuades the target to make a payment under false pretenses, make up 40 percent of payment fraud. For context, payment fraud was 40 percent of ALL crime reported in the UK in 2023.

So since October 7, 2024, the UK Payment Systems Regulator has required banks sending and receiving funds to share the costs of reimbursing consumers who are victims of APP fraud, up to a limit of £85,000 ($102,000). This creates strong incentives for banks to detect and prevent fraudulent payments and improve customer education. Regulators in the US, Australia, Singapore and other jurisdictions are also stepping up their efforts to combat fraud.

In November 2024, the UK Information Commissioner's Office (ICO) called on organizations to share with banks information that might help prevent fraud. In the European Union, Payment Services Directive 3 (PSD3) and Payment Services Regulation 1 (PSR1) are set to take effect in 2026, making financial institutions liable for fraud, obliging them to verify payees, improve customer authentication and – no less important – share fraud intelligence with peers.

Collaborative detection



While awareness campaigns are encouraging consumers to focus on digital hygiene and regulators are beginning to require banks to compensate customers for fraudulent transactions that slip through, collaboration will be key to beating the scammers.

International regulations are already in force across many jurisdictions requiring banks to know their customers and strive to prevent cross-border money laundering. This collaboration has been so successful that fraudsters have resorted to domestic money mules to launder their gains.

To tackle money mule transactions and networks, regulators are encouraging payment service providers (PSPs) to share more data and strengthen detection tools.

With instant payments becoming the norm, flagging and pausing suspicious transactions in real time is crucial. Central monitoring and hold mechanisms are now widely used and effective, allowing PSPs to identify doubtful transactions, hold them and reconfirm with customers through secure out-of-band channels.

NetGuardians' Instant Payments solution uses advanced analytics, AI-driven profiling and real-time detection to secure transactions without sacrificing speed or customer experience.

Customers may find confirmation calls an inconvenience. But ultimately, they will reward banks that save them from fraudsters with loyalty and satisfaction.

At NetGuardians, we believe that sharing information about fraud is the key to improving prevention. We are already encouraging voluntary sharing of fraud insights between financial institutions, making it harder for crooks to switch banks to avoid being caught out. Banks and their crime-fighters don't need to wait for regulators to compel action. We believe they should act now to implement advanced analytics and data-sharing frameworks to put pressure on mule schemes, enhance fraud detection and protect their customers.


100
FEDERAL RESERVE NOTE
LG 14832266 E
G7
UNITED STATES FEDERAL RESERVE SYSTEM
Secretary of the Treasury.
Treasurer of the United States.
100
FRANKLIN

NetGuardians

About NetGuardians

NetGuardians is an award-winning Swiss FinTech helping financial institutions in over 30 countries to fight fraud. More than 100 banks and wealth managers, including 45 percent of all Swiss cantonal banks and three of the top 10 private banks as ranked by Euromoney, rely on NetGuardians' 3D artificial-intelligence (3D AI) solution to prevent fraudulent payments in real time.

Banks using NetGuardians software have achieved an 85 percent reduction in customer friction, enjoy more than 75 percent lower operating costs and have detected new fraud cases. NetGuardians is the fraud-prevention partner of major banking software companies, including Finastra, Avaloq, Mambu and Finacle. Headquartered in Switzerland, the FinTech has offices in Singapore, Kenya and Poland.

Our offices

NetGuardians Headquarters

Avenue des Sciences 13
1400 Yverdon-les-Bains
Switzerland
T +41 24 425 97 60
F +41 24 425 97 65

www.netguardians.ch
info@netguardians.ch

NetGuardians Asia

WeWork
Robinson Road 71, #14-01
Singapore 068895
T +65 6224 0987

NetGuardians Africa

The Mirage Tower 1, 12th Floor
P.O. Box 574 – 00606 Sarit
Waiyaki Way, Nairobi
T +254 796 616 263