NetGuardians

The Top Banking Fraud Types to Watch in 2022

Introduction

Banking fraud is constantly evolving as conditions change, creating new vulnerabilities for banks and opportunities for fraudsters. Staying abreast of this moving target is essential if banks are to find solutions that can spot and prevent such scams, especially given the effects of the pandemic on the banking fraud landscape.

In its report The Next Normal: Preparing for a Post-Pandemic Fraud Landscape, published in December 2021, the Association of Certified Fraud Examiners found that 51 percent of respondents had uncovered more fraud since the start of the pandemic. Some 71 percent expected the level of fraud impacting their organization to increase over the next 12 months. The most serious areas of concern for the coming year were cyberfraud, including business email compromise, and social engineering where 82 percent of respondents expected an increase.

Our review of Top Banking Fraud Types to Watch in 2022 highlights the common methods criminals use to defraud banks and their customers – something everyone should know about going forward. We classify the different types of frauds according to whether the payment is initiated by unauthorized or authorized parties. In our view this is the most relevant classification system to use, since this distinction directly affects the level of liability that banks face.

We also present recent case studies for the different fraud types, based on cases that have been detected and prevented by NetGuardians software in deployments with banks around the world.

Why banking fraud has accelerated

Over the past two years, the Covid-19 pandemic has created ideal conditions for many types of payment fraud to proliferate. Millions of people have been forced to change their everyday behavior, especially the way they work, shop and communicate, turbo-charging fraud in the following ways:

- The shift to remote working among many office staff, including bank employees, has required people to access corporate systems remotely – often with limited security measures in place. Some internal controls and confidentiality requirements have also become harder to enforce in the home-working environment.

- A sudden, further shift of banking transactions onto digital channels as branches and stores close has meant banks have switched to digital and telephone channels to keep services open. This is especially the case in the developing world, where banks have moved fast to embrace digital innovation, but in some cases have neglected the security element. Transaction limits on digital channels have been increased, for example, meaning account takeover can now result in bigger thefts.

- The explosion of home delivery for retail purchases has created new opportunities for phishing scams involving email or text alerts, as well as the general increase in communications via digital channels that can be faked and exploited for phishing purposes.

- The huge increase in retail participation in financial markets during lockdowns has created scope for online investment.

Although the pandemic has boosted the number of opportunities open to fraudsters, the way they operate has not changed nearly as much. Although criminal gangs that hire skilled staff on the dark web to deploy hi-tech tools are responsible for some frauds, many others remain extremely low-tech. Many frauds are successfully executed using familiar tools such as email, phone calls and messages over social media. They rely on little more than social engineering and well-known psychological tricks to manipulate and dupe their victims.

Most bank frauds target banks' customers. But Covid-19 has also allowed internal banking fraud and corporate fraud to grow. The conditions that support internal fraud, as set out in the Fraud Triangle devised by Donald Cressey, are all in place in the current environment:

- **Pressure** – many employees may be facing redundancy or a salary freeze as their company attempts to weather the effects of the pandemic on their business.

- **Opportunity** – remote working may create gaps in internal controls that make it easier for insiders who know the system's weaknesses to execute their plans.

- **Rationalization** – employees tempted to defraud their employer may convince themselves that their actions are justified because they are working hard in difficult circumstances but receiving little or no reward or recognition.

Most bank frauds target banks' customers. But Covid-19 has also allowed internal banking fraud to grow.

In the developing world, the introduction of improved security for transactions via digital channels, such as one-time passwords for mobile banking, has prompted criminal gangs to seek alternative routes. This has led to greater recruitment of insiders to facilitate fraud as their access to the bank's back-end systems opens a new avenue for fraud attacks. While these are low volume, they typically attempt to steal sizeable sums.

The 2022 Fraud Landscape

Our survey of the 2022 payment fraud landscape classifies frauds according to who initiates the payment – an authorized or unauthorized party. Both types tend to involve a combination of technology tools and efforts to manipulate and dupe the victim.

However, in almost all cases, the fraud is executed by initiating payments or withdrawals from victims' accounts that are not consistent with their normal patterns of behavior. This is the weakness in such fraud attempts that enables NetGuardians' AI software to identify and prevent them.

P04 **Unauthorized frauds**

1. Bank insider
2. Phishing
3. Man in the middle/pharming
4. Technical support
5. Mobile SIM swap
6. Account takeover

P12 **Authorized frauds**

1. Push payment social engineering
2. Romance scams
3. Business email compromise
4. Invoice fraud
5. Investment scams

Fraudulent Payments Initiated by Unauthorized Parties

1. Bank insider frauds

Insiders can be bank employees or staff employed by IT vendors working with the bank. Because these people have detailed knowledge of the bank's internal systems, this fraud can be difficult to detect and can continue for long periods unless a robust fraud-monitoring system is in place.

Insiders exploit user privileges to access victims' accounts directly, or to transfer funds from the bank's internal payment accounts into accounts belonging to customers. The funds are then transferred to external bank accounts controlled by the fraudster or to pre-paid cards. These types of cards are popular with fraudsters because they are issued with few "know your customer" (KYC) checks and can be used to make multiple currency cash withdrawals. They can also be used for "card not present" transactions which normally have a higher transaction limit.

In its 2020 benchmarking report Fraud in the Wake of Covid-19, the ACFE revealed that 48 percent of banks and financial service providers had seen an increase in internal fraud. Shockingly, 71 percent expected it to increase further, with almost a quarter expecting a "significant" increase.

CASE STUDY

Privileged user abuse

An IT administrator at a bank in Tanzania took advantage of back-end user privileges to inflate account balances for an accomplice by a total of $22,000. The intention was to withdraw the funds from ATMs and via mobile banking, but the fraud was detected and the money never left the bank.

Solution: The software detected that the privileged user checked the accomplice's account several times over a period of days and flagged the behavior as suspicious.

2. Phishing scams

Millions of fake official emails or text messages from banks, companies, delivery agents, tax authorities, health services, and many other sources are sent every day. The emails contain links that, once clicked by an unwary victim, automatically download and install a piece of malware on their device which gathers personal information needed for an account takeover.

At least one person in 86% of organizations clicked a phishing link during the Covid-19 lockdowns, according to Cisco's 2021 cybersecurity trends report. The company suggests that phishing accounts for 90% of data breaches.

The UK banking industry body UK Finance reported in May 2021 that three-quarters of financial services firms had seen an increase in digital crime since the pandemic began. The UK's National Cyber Security Centre said it had taken down more scams in the first year of the pandemic than during the previous three years combined.

CASE STUDY

Phishing-enabled account takeover

A fraudster used phishing to introduce malicious code into the Swiss victim's computer and acquired their e-banking credentials. The criminal then took over the victim's account and attempted to make an illicit transfer of CHF 19,990.

Solution: NetGuardians stopped the payment as several factors did not match the customer's profile, including the size of the transfer, the new beneficiary and bank account used, as well as the unfamiliar screen resolution and browser employed by the fraudster.

Phishing is also frequently used to carry out business email compromise (BEC) frauds. Fake official emails or text messages from banks, companies, delivery agents, or even health authorities claiming to send Covid-19 test results, persuade the victim to click on a link. A banking Trojan or malware is then installed on the victim's device, allowing the fraudsters to take control of the victim's e-banking.

3. Man in the middle/pharming scams

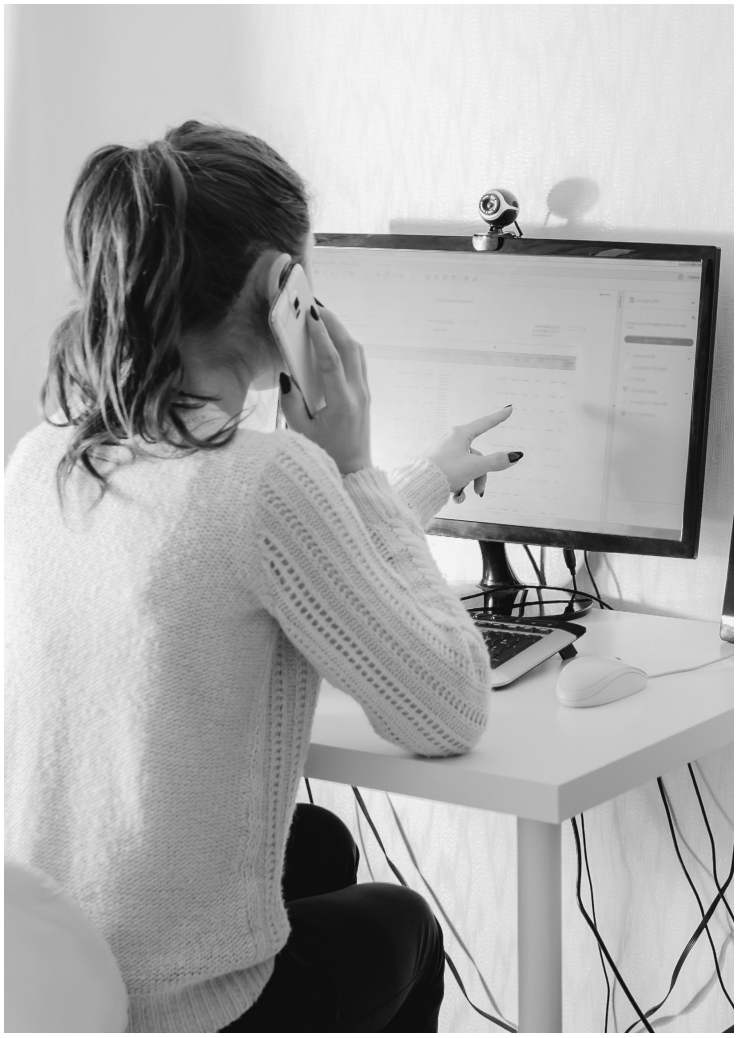
A hacker obtains sensitive information transmitted between two other parties online. This can happen when the victim is intercepted trying to log in to their online or mobile banking service, allowing their log-in information to be harvested.

CASE STUDY

Man in the middle scam uses fake QR code

A client wanted to access her e-banking service. After entering her credentials and scanning the QR code, a message appeared in French and German asking her to re-enter her credentials for greater security. After she did so, an error message appeared saying the site was unavailable. This is likely to have been a man in the middle attack in which the second QR code was displayed by a hacker to recover the victim's account credentials. The fraudster then attempted a payment of CHF 38,000.

Solution: NetGuardians blocked the payment due to unusual session information, including browser language and screen resolution, and transaction details including the unusual amount and beneficiary bank. The system logs showed three sessions that raised suspicions, suggesting the fraudster accessed the victim's account several times while attempting the payment.



4. Technical support scam

Fake technical support staff call the victim, who is told that there is a problem with their software. The victim is duped into giving the caller control of their computer remotely, sometimes with the help of personal information about them gathered via social engineering. The fraudster is then able to gain access to their computer and steal confidential information. Alternatively, the victim receives an email or is invited to click on a pop-up window.

Research published by Microsoft in July 2021 found that the proportion of respondents who had experienced technical support scams had declined since 2018, but the proportion that lost money through these frauds increased from 6% in 2018 to 7% in 2021.

CASE STUDY

Technical support scam

The fraudster impersonated a Microsoft tech support worker and called the victim. Through social engineering, the perpetrator managed to obtain enough information about the victim's e-banking credentials to attempt to transfer $7,500 to an illicit account in Lithuania.

Solution: NetGuardians' AI risk models stopped the transaction because its features did not match the customer's profile, including the unusual currency, type of transaction, beneficiary account details, and country of destination.

5. Mobile SIM-swap frauds

Stealing mobile numbers via SIM swap is a key fraud vector in the developing world, because the primary way most people access mobile banking is via their mobile phone number. Their mobile number is connected to their bank account and is used to verify their identity – most banks also use this phone number as the primary 2FA implementation mechanism.

The victim receives a call from a fraudster pretending to represent a telco to check account details. Using the personal information obtained, the fraudster poses as the victim and contacts their mobile service provider to have their number transferred to a new SIM in a device the gang controls. This gives access to the victim's mobile wallet and can even allow the fraudster to attempt to reset the victim's mobile banking security data and access their account. In other cases, gangs work with insiders at telco sales teams to obtain replacement SIMs for "lost phones." According to the South African Banking Risk Information SIM-swap frauds increased 91% during 2020. SIM-swap frauds have also been used around the world to access crypto wallets. The potential gains from cryptocurrency are huge as it is decentralized, can easily be anonymized and has real monetary value.

CASE STUDY

M-wallet fraud in Africa

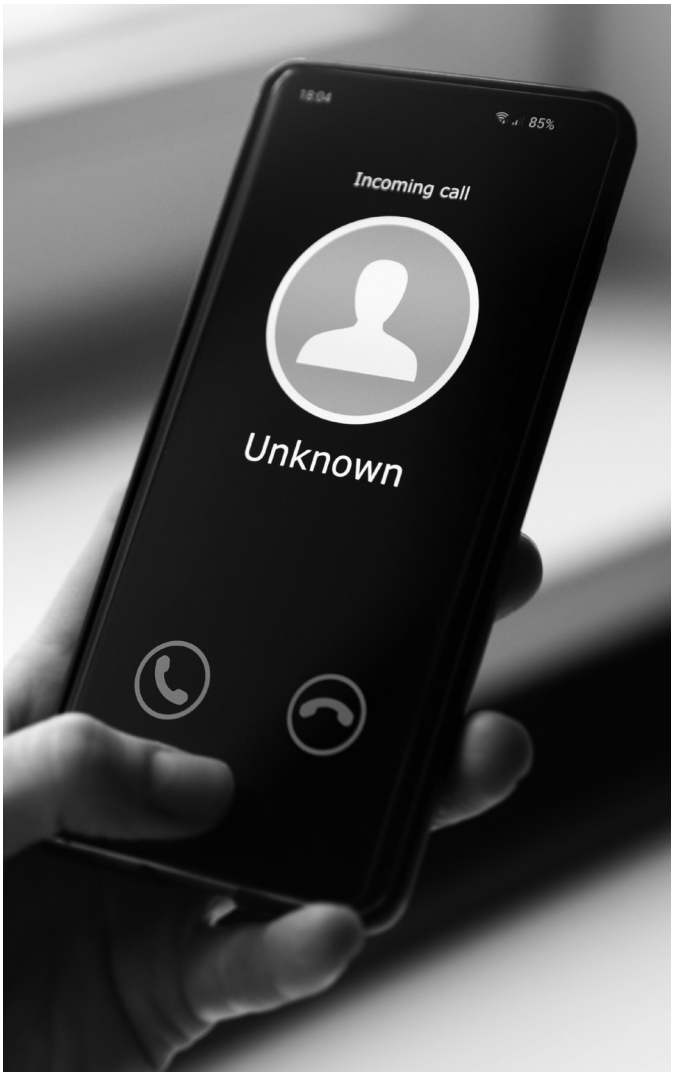
In one recent case reported in Kenya, a gang targeted well-off people who had recently died, aiming to cancel and swap their SIM to a new device before their family had the chance to access the deceased person's bank account and establish their exact wealth. Once the SIM was transferred, the victim's mobile wallet was emptied and the funds transferred to other wallets, from where it was withdrawn. A second SIM-swap gang had more than 10,000 SIM cards when police arrested them in October 2020.

Solution: NetGuardians' fraud software can spot and prevent attempts to withdraw funds stolen during this type of fraud. Repeated visits to the same ATM in quick succession raises an alert in real time, enabling the bank to check whether or not the attempted withdrawals are legitimate.

6. Account takeover resulting from social engineering and telephone scams

Even well-known, unsophisticated techniques such as telephone frauds, which date back decades, continue to be extremely effective, especially when combined with basic social engineering using information about the victim that is easily found online.

This type of scam can involve callers pretending to be agents working for a wide variety of organizations, such as the victim's bank or the tax authorities. Victims are persuaded to disclose their banking credentials, allowing the criminals to take control of their account.



CASE STUDY

Account takeover

A fraudster impersonating a bank employee persuaded a customer to disclose their e-banking login details through social engineering. The fraudster then took over the account and attempted to transfer £21,000 to an illicit account.

Solution: AI-based risk monitoring software blocked the transaction due to unusual e-banking and transaction characteristics, including the unusual amount, screen resolution, beneficiary bank and account details, e-banking session language, and currency.

Even well-known, unsophisticated techniques such as telephone frauds continue to be extremely effective, especially when combined with social engineering.

Fraudulent Payments Initiated by Authorized Parties

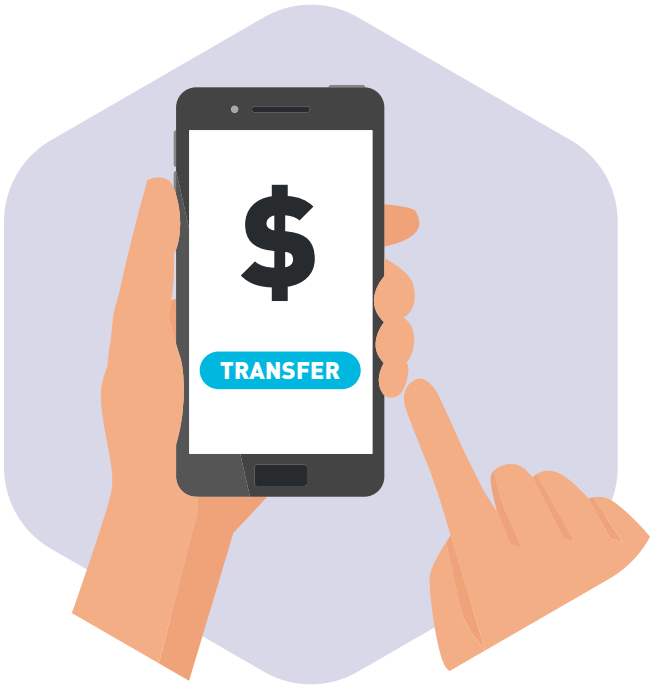
1. Authorized push payment fraud resulting from social engineering

Social engineering and simple telephone impersonation techniques can also be used to dupe victims into making payments to accounts controlled by the fraudsters themselves. For example, victims may be told that their account has been compromised and they must transfer their money to a new account to prevent it from being stolen.

According to the UK banking industry trade body UK Finance, £479 million was lost to authorized push payment fraud in 2020, up 5 percent on 2019. The number of fraud incidents rose 22% year-on-year.

CASE STUDY

Authorized push payment fraud



Using impersonation techniques, the fraudster convinced the bank customer to transfer €125,000 to an illicit account in Spain.

Solution: AI-based monitoring software blocked the transaction because certain variables did not match the customer's profile, including the date the transfer was initiated, the destination country, beneficiary account, order type, and currency.

2. Romance scams

The victim is approached via text message, email or social media and convinced to begin a long-distance relationship. Once the victim is drawn in, the fraudster requests money transfers to allow them to come to the victim's country, clear debts or unlock a frozen bank account. Even after these attempted frauds are flagged up by their bank, victims often insist on authorizing the payments. This demonstrates the power of romance scams to dupe victims, who want to believe they have found a genuine relationship. Banks need to be able to show victims that the payment is going somewhere other than what the victim has been told.

According to the US Federal Trade Commission, romance fraud has mushroomed in recent years. In 2017, 17,000 victims reported losing $87 million, but by 2021 the number of victims had grown to 56,000 and losses totalled $547 million. The New York Times cited the example of a 76-year-old widow who transferred more than $660,000 to bank accounts she thought belonged to a US Army general in Afghanistan. In Singapore, the police force's Anti-Scam Centre says that across all the cases it has investigated since June 2019, love scams accounted for nearly half the total amount that fraudsters had attempted to steal.

CASE STUDY

Romance scam

The fraudster introduced himself to the victim as an American soldier based in the Middle East. A romantic relationship began and the fraudster convinced the victim to make three transfers to his bank in Germany – of $1,500, €3,000, and €11,300.

Solution: NetGuardians' AI risk models stopped the first and third transactions, spotting unusual variables, including the beneficiary bank account, the destination country, the amount and currency.

3. Business email compromise (BEC)

Fraudsters frequently target companies by impersonating a senior executive. An email is sent to an employee, either from the victim's own email account, which has been hacked, or from a spoofed email address. The email is often followed by a call apparently from the CEO, a senior executive, or from a bogus law firm or consultant, telling the employee who received the email to respond immediately. Deep fakes are increasingly used for video or voice calls. The email usually requests a large payment to a fake account in connection with an urgent or sensitive issue such as an acquisition.

The US Federal Bureau of Investigation says that between June 2016 and July 2019 it received more than 166,000 reports of email compromise, with total losses of more than $26.2 billion.

CASE STUDY 1

CEO fraud

A fraudster impersonated the CEO of a Spanish company and over email convinced an employee to transfer €170,000 to an illicit account.

CASE STUDY 2

BEC fraud

The victim received an email from their business partner's email account, which had been hacked, requesting a transfer of $100,000 to an account in Peru.

Solution: In both cases, NetGuardians' risk models blocked the transactions due to the unusual variables the transactions exhibited, including the beneficiary account details, destination country, operation type, order type, and currency.

4. Invoice frauds

Invoices purporting to come from a genuine supplier are emailed to the company, along with fake account details for payment. This type of fraud can cause major problems for smaller companies that lack the controls to prevent them and rely on non-specialist, junior staff to make payments.

CASE STUDY

Invoice fraud

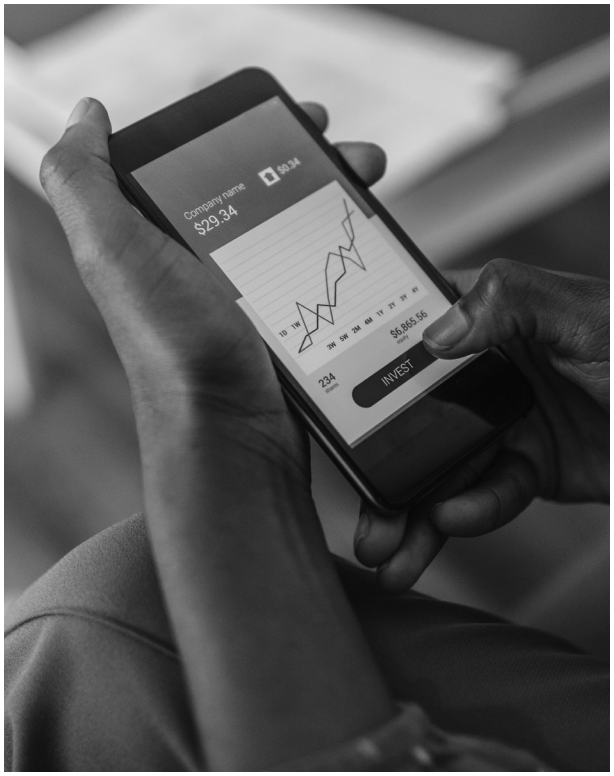
A company received an invoice for US$69,000 payable to a previously unknown account in Singapore. The Singapore-based beneficiary's name was similar to the name of an existing supplier based in Hong Kong. The IBAN shown on the fake invoice had been modified.

Solution: NetGuardians' risk monitoring software detected and blocked the fraud due to the unusual amount, destination country, and bank.

5. Investment scams

The number of individuals investing online has grown strongly during the Covid-19 pandemic, partly due to home working. In response, gangs have set up fake investment websites to fool people looking to invest in stocks, commodities, and cryptocurrencies. The sites are marketed to victims using phishing emails and online adverts on social media sites.

In January 2021, the UK's Financial Conduct Authority warned that more than £78 million had been stolen from UK investors during 2020 through "clone firm" investment scams involving fake websites and documents that imitated legitimate companies. Reports of these clone firm scams rose by 29 percent between March and April 2020, when the UK went into its first lockdown. The average loss reported by consumers was more than £45,000.



CASE STUDY

Investment fraud

The victim was advised by a fraudster impersonating a business partner to invest in a fictitious company and ordered a payment of $170,000 to an account at a bank in Bulgaria.

Solution: The monitoring software blocked the payment because several variables did not match the victim's profile, including the unusual destination country, bank, beneficiary account, amount, and currency.

During the Covid-19 pandemic gangs have set up fake investment websites to fool people looking to invest in stocks, commodities, and cryptocurrencies.

Conclusion

Banking frauds are constantly shifting as criminals find effective ways to get past their victims' defences. Recently, for example, fraudsters are reported to be contacting people about Covid vaccination appointments and trying to get them to divulge confidential information. The huge rise in home delivery of goods during lockdowns has created a new line of attack for fraudsters.

Text messages purporting to come from Amazon invite people to click on a link to obtain a refund. As always, fraudsters will "follow the money" and move to those channels where the number of potential victims is increasing.

No matter how mechanisms for executing the fraud change shape, however, they will still rely for their success on the

same basic aspects of human psychology. Fraudsters will succeed, as they always have, by exploiting their victims' fear, anxiety and readiness to trust messages that appear to come from official sources.

Banking fraud continues to increase and the question of who is liable for the losses that result is becoming a more serious concern. Banks are generally liable to reimburse victims of frauds in which the fraudster initiates the illicit payment. In cases where the victim does so – authorized push payment frauds – banks have usually been able to avoid liability.

This is changing, however. In the UK, nine leading banks have voluntarily signed up to the Contingent Reimbursement Model Code, which allows individuals, micro-

enterprises and charities that become victims of authorized push payment fraud to claim reimbursement from their bank – unless the victim was warned about the potential for scams before making the payment but chose to go ahead in any case. This greatly increases the banks' exposure to fraud risks and makes it even more important for them to take effective real-time prevention measures that will allow suspect transactions to be blocked and validated.

Although a wide variety of banking frauds are commonly attempted, there is only one reliable way to detect and prevent them: comparing the fraudulent transaction against the historical pattern of behavior associated with the account holder or system user. This is why in creating solutions it is critical to focus not on the different types of fraud but on the usual behavior of the account holders, so that anomalies can be detected and flagged.

NetGuardians' AI-based anti-fraud software monitors all account transactions and evaluates them against the established behavioral profile linked to the account holder or his or her peers. This enables the system to highlight transactions that are inconsistent with the known user's profile and flag them to security staff so that fraudulent payment requests and withdrawals can be blocked.

Anomalies and AI algorithms

The system carries out checks on transactions across multiple axes. It tracks unusual access to the bank's internal systems and monitors internal users' actions where these are linked to suspect transactions.

The software also uses AI algorithms to identify unusual activity on customers' accounts that may indicate account takeover. Triggers may include the detection of a different screen resolution than the one expected on the login device, a login from a new device or a previously unknown location, a login from an unknown browser, or use of a different language. "Velocity models" are employed to flag heightened activity on customer accounts, for example when multiple transactions are initiated in quick succession, which may indicate an attempt to empty the account as rapidly as possible.

Reducing false alerts and operational losses

All anti-fraud systems produce false positives that have an impact on customer satisfaction and lead to unnecessary customer call-backs. However, constant R&D efforts are improving the precision of the machine-learning algorithms that power NetGuardians' systems, leading to improved detection rates and reduced inconvenience for customers.

These efforts have achieved impressive results: a reduction of up to 85 percent in false-positive alerts, a reduction of up to 93 percent in time spent investigating fraud, and a more than 75 percent cut in operating costs related to fraud mitigation.

Ultimately, this approach is the only practical solution to protecting customers, eliminating false positives, and stopping emerging types of fraud that would otherwise be extremely difficult to detect.

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

NetGuardians Asia
WeWork | NetGuardians
71, Robinson Rd, #14-01
Singapore 068895
T +65 6224 0987

NetGuardians Africa
The Mirage, Tower 2,
Pentfloor Waiyaki Way,
Westlands P. O. Box
100240-00101 Nairobi, Kenya
T +254 709678 005

www.netguardians.ch
info@netguardians.ch

ABOUT NETGUARDIANS

NetGuardians is the only company to combine unsupervised, supervised and adaptive learning to create 'Smarter 3D AI' - a flawless fraud detection system that is always learning to help financial organizations match the evolving speed and intelligence of cyber criminals.

More than 80 banks worldwide, including UOB and Pictet & Cie, rely on NetGuardians' 3D artificial intelligence (3D AI) solution to prevent fraudulent payments in real time. Its ready-to-go solutions help financial institutions to spot and stop fraudulent payments from day one.

Banks using NetGuardians' software have achieved reductions of up to 85 percent in false positives, decreased the cost of their fraud prevention operations by an average of 75% and have detected new fraud cases.

NetGuardians is the fraud-prevention partner of major banking software companies, including Finastra, Avaloq, Mambu, and Finacle.

The company was listed as a representative vendor in Gartner's 2020 Market Guide for Online Fraud Detection and Global Leader in the Aite's 2021 Fraud and AML Machine Learning Platforms Report.

Headquartered in Switzerland, NetGuardians has offices in Singapore, Kenya, and Poland.

For further information, questions, and feedback, please contact us.

NetGuardians