BioCatch

2024 Digital Banking Fraud Trends in EMEA

BioCatch report on the current online fraud landscape in Europe, the Middle East, and Africa, with regional case study and analysis.

March 2024

About This Report

To compile this report, BioCatch's team of experts, led by its worldwide advisory team and threat analysts, conducted research using data from both BioCatch customers with active deployments in the EMEA region and official sources in the region.

This report offers a comprehensive perspective on the current threat landscape and banking fraud trends in EMEA, an analysis of the evolution of the fraud landscape across the region, and a deep-dive case study into the different uses of remote access tools.

This report is presented in the following sections:

- Key Fraud Trends in EMEA
- Threat Landscape in EMEA
- Evolution of the Fraud Landscape
- Deep Dive: Differentiating Active and Passive RAT

Key Fraud Trends in EMEA

Social Engineering is the main focus across Europe, particularly voice scams.

While banks in the UK devoted much of their focus to **voice scams** over the last few years, BioCatch data now shows a 25% decline in that type of fraud in the UK in 2023 – a finding shared by industry bodies. This data suggests banks' efforts to curb these scams with additional controls – including behavioural biometric intelligence – is starting to yield results.

With UK banks doing more to stop voice scams, BioCatch data shows fraudsters pivoted to new versions of **Account Takeover (ATO) fraud**. We saw more cases of the **patient fraudster** in the UK in 2023, whereby the bad actor attempted to exploit existing controls that look at device usage by regularly logging into an account to earn the bank's trust before making fraudulent payments. Such cases led ATO's slice of the total fraud pie to grow by 13% last year.

Stolen device cases are appearing more frequently in several countries, with a 43% increase seen in cases reported to BioCatch.

Continued focus on identifying **mule accounts** in anticipation of PSD3 and PSR, with banks creating new organizational capabilities to better detect and manage them.

75% reported frauds from mobile devices, up 6% compared to 2022

25% decrease in reported voice scams year-over-year in the UK

10K+ bad accounts alerted by BioCatch's Mule Account Detection solution

Threat Landscape in EMEA

Benelux

- Traditional phishing and new 'quishing' attacks via malicious QR codes
- Voice scams, including bank impersonation, help-desk frauds, and false job advertisements
- Some high-profile deep fake cases

United Kingdom

- APP scams
- Patient fraudster cases, whereby fraudster regularly logs in to accounts, building trust before making payment
- Remote access for both ATO and scams
- Stolen devices
- Mule accounts

France

- Phishing
- OTP vishing
- Remote access
- Bank impersonation scams

Italy

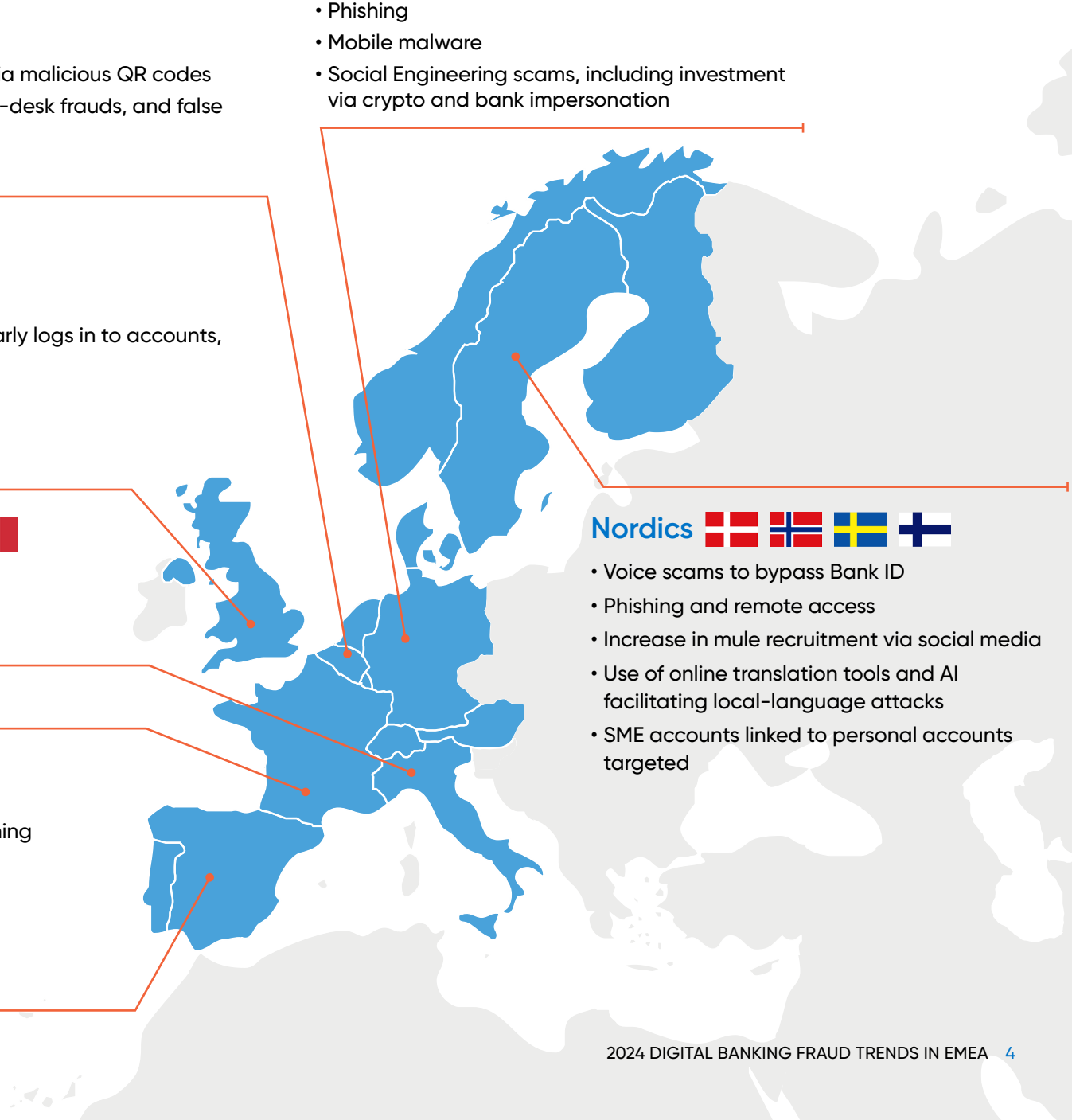
- Phishing
- ATO
- Scams

Spain/Portugal

- ATO using stolen credentials from phishing/smishing attacks, including the use of mobile malware
- Help-desk frauds using RAT
- Stolen devices
- Increased focus on social engineering scams, mainly bank impersonation

DACH

- Phishing
- Mobile malware
- Social Engineering scams, including investment via crypto and bank impersonation



Nordics

- Voice scams to bypass Bank ID
- Phishing and remote access
- Increase in mule recruitment via social media
- Use of online translation tools and AI facilitating local-language attacks
- SME accounts linked to personal accounts targeted

BioCatch

Evolution of the Fraud Landscape

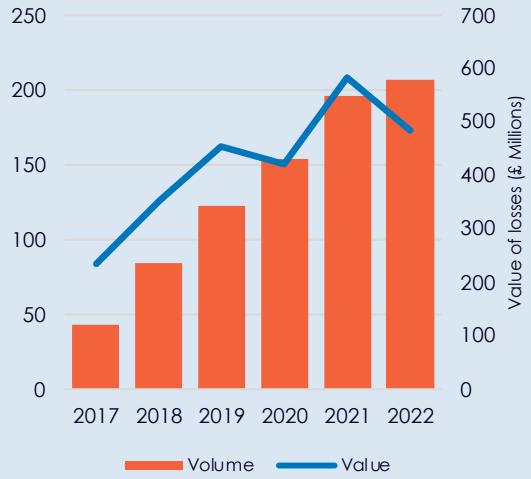
EMEA continues to see evolution in the digital banking attacks that started in the UK around five years ago, with authorised fraud (i.e., social engineering scams) overtaking unauthorised fraud (ATO) in many countries.

By using a wider range of lures (bank impersonation, purchase, romance, investment, etc.), fraudsters have launched more attacks that have stolen more money. Increasingly, we also see artificial intelligence (AI) tools facilitating attacks in native languages.

UK Fraud Cases & Losses

Unauthorised frauds across all platforms continuously increased, reaching its peak in 2021. After this, there has been a significant drop.

UK Social Engineering Cases & Losses



Cases of APP fraud have continually risen, becoming the main fraud type in volume and value since 2019.

The UK landscape has shifted to a space where social engineering scams became the main source of fraud losses in 2019. Over time, this has increased, and we see fraudsters attempting more low-value payments in an attempt to bypass bank controls for scams. As a result, more needs to be done to protect customers.

EVOLUTION OF THE FRAUD LANDSCAPE:

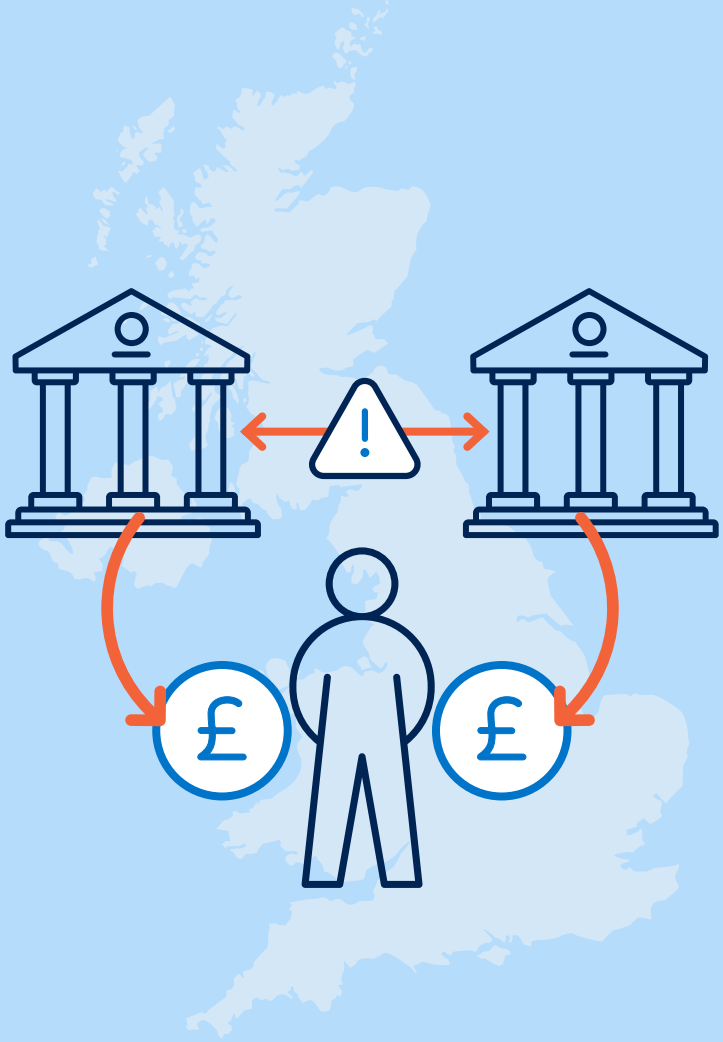
A Changing Landscape

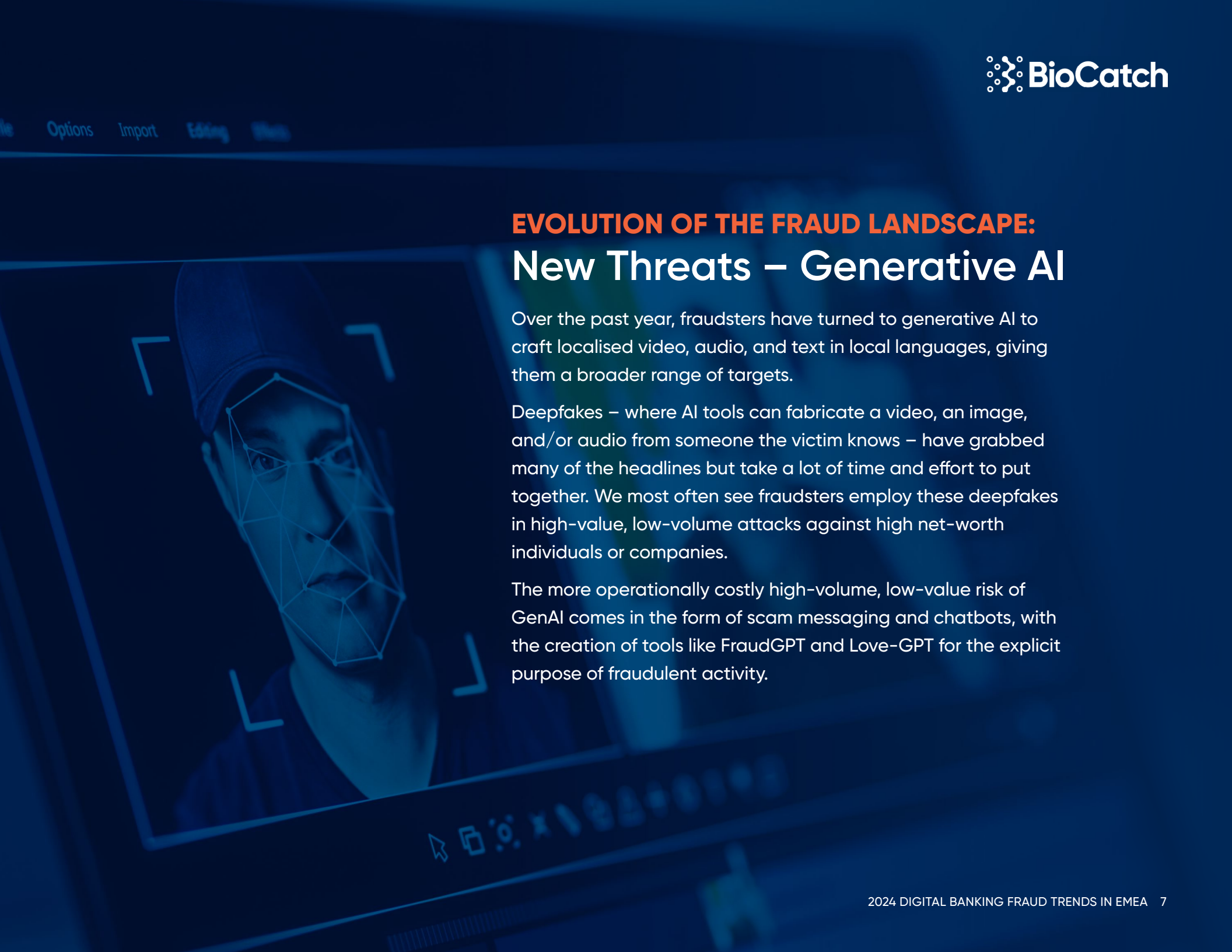
The revolution in the region comes in the regulatory response to scams. The UK became the region's first country to mandate reimbursement for victims, irrespective of scam type. Even more revolutionary:

Reimbursement in the UK splits liability between the sending and receiving banks. In just 18 months, this has galvanised mule-detection capabilities in the UK.

Within the EU, the EBA is also moving in this direction, by including reimbursement for specific impersonation scams in the draft proposal for PSD3, as well as requiring reimbursement for unauthorised attacks. This legislation, however, would hold only the sending bank liable for fraudulent transactions – similar to what some European countries (most notably, the Netherlands) already do.

"With banks increasingly on the hook to reimburse fraud victims, they've made it more difficult for fraudsters to take over accounts. Scammers have thus turned to social engineering to bypass bank controls via authorised frauds."





EVOLUTION OF THE FRAUD LANDSCAPE:

New Threats – Generative AI

Over the past year, fraudsters have turned to generative AI to craft localised video, audio, and text in local languages, giving them a broader range of targets.

Deepfakes – where AI tools can fabricate a video, an image, and/or audio from someone the victim knows – have grabbed many of the headlines but take a lot of time and effort to put together. We most often see fraudsters employ these deepfakes in high-value, low-volume attacks against high net-worth individuals or companies.

The more operationally costly high-volume, low-value risk of GenAI comes in the form of scam messaging and chatbots, with the creation of tools like FraudGPT and Love-GPT for the explicit purpose of fraudulent activity.

EVOLUTION OF THE FRAUD LANDSCAPE:

Combining Fraud and AML Efforts

The UK's requiring of banks to reimburse defrauded customers has drawn into focus a piece of the fraud value chain ignored for too long: the mule. Every single fraud requires a mule account to receive the stolen funds and enable the fraudster to cash out.

Romance, investment, and purchase scams are difficult for banks on the sending account side to detect, leading some banks to focus more on the receiving account. Financial institutions are creating new teams to proactively identify mule accounts. Most have realised the earlier in the value chain they can identify a scam, the lower the operational cost of dealing with both the mule and any reimbursement. To proactively identify mules, banks must spot changes in account holder behaviour (when an account is sold, when it's accessed through a new device, when the human behind it starts behaving differently, etc.).

In 2024, we expect to see wider adoption of risk management techniques within the AML/mules space. AML, driven by the need to spot mules, is going to evolve from compliance-driven retrospective analysis to real-time identification of bad accounts (and the networks behind them). The key to this will be more utilisation of digital data within AML teams, and an increase in data sharing. Some regions such as Sweden are already sharing for AML, and others will follow. The next step is to provide a view of the accounts on both sides of a transaction to gauge the trustworthiness of it. More advanced profiling of account and user risk driven by AI is where the industry is heading.

"The earlier in the value chain banks can identify a scam, the lower the operational cost of dealing with both the mule and any reimbursement."

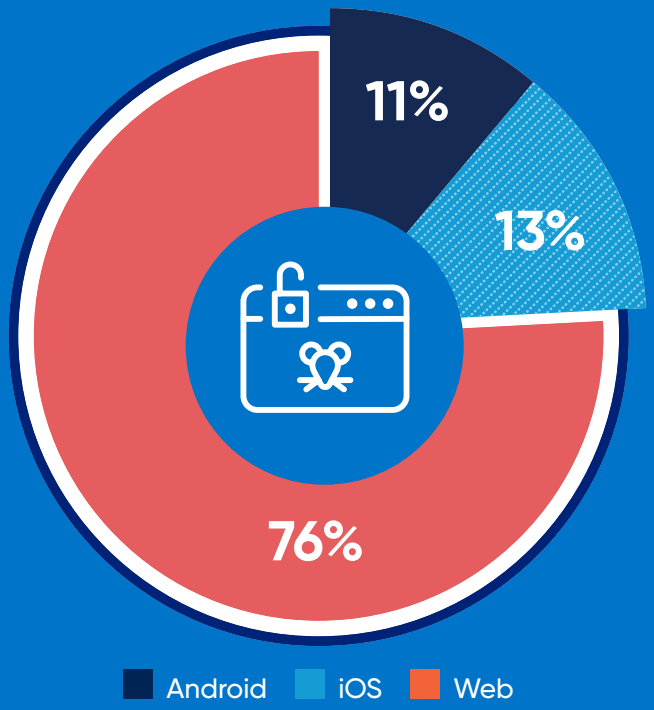
BioCatch

DEEP DIVE:

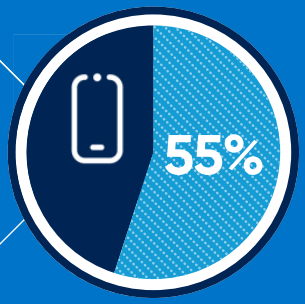
Differentiating Active and Passive RAT

When investigating cases, we came across an interesting trend with regards to remote access, and how we can interpret cases reported as remote access frauds, depending on the device they originate from. This case study will explore our findings and conclusions.

Reported Remote Access Fraud



24% remote access cases takes place on a mobile device



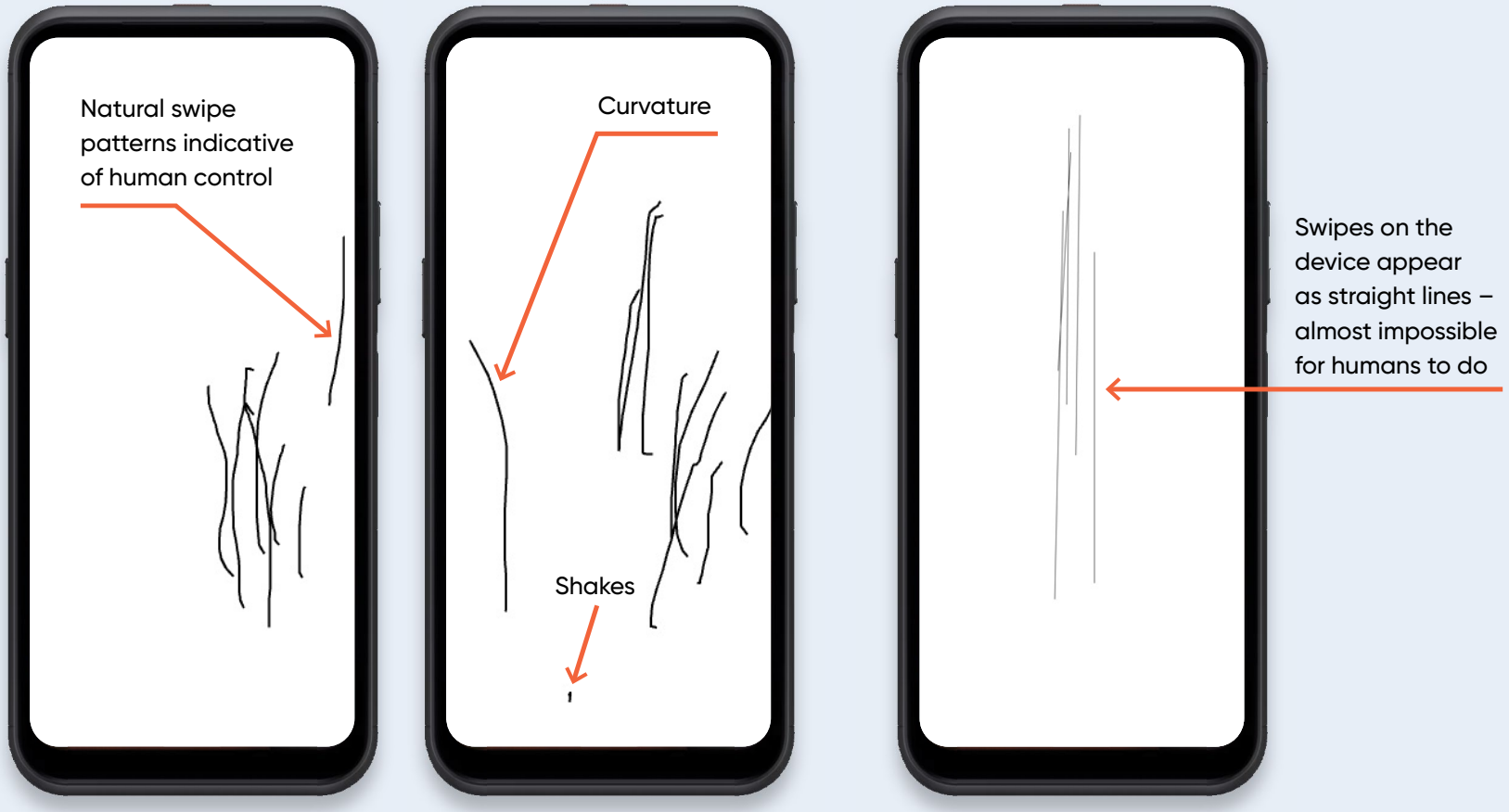
55% of these are from an iOS device

In theory, iOS still do not allow for a user's device to be controlled via remote access, limiting the functionalities of apps like AnyDesk or TeamViewer to mere screen sharing. This means that any fraud case involving remote access would imply that the victim is sharing their screen but carrying out all actions themselves, under the guidance of the fraudster.

ACTIVE/PASSIVE RAT:

Screen Activity

The images below show the user interaction during three sessions; two from iOS devices and one from an Android device.



Activity concentrated around user's dominant hand

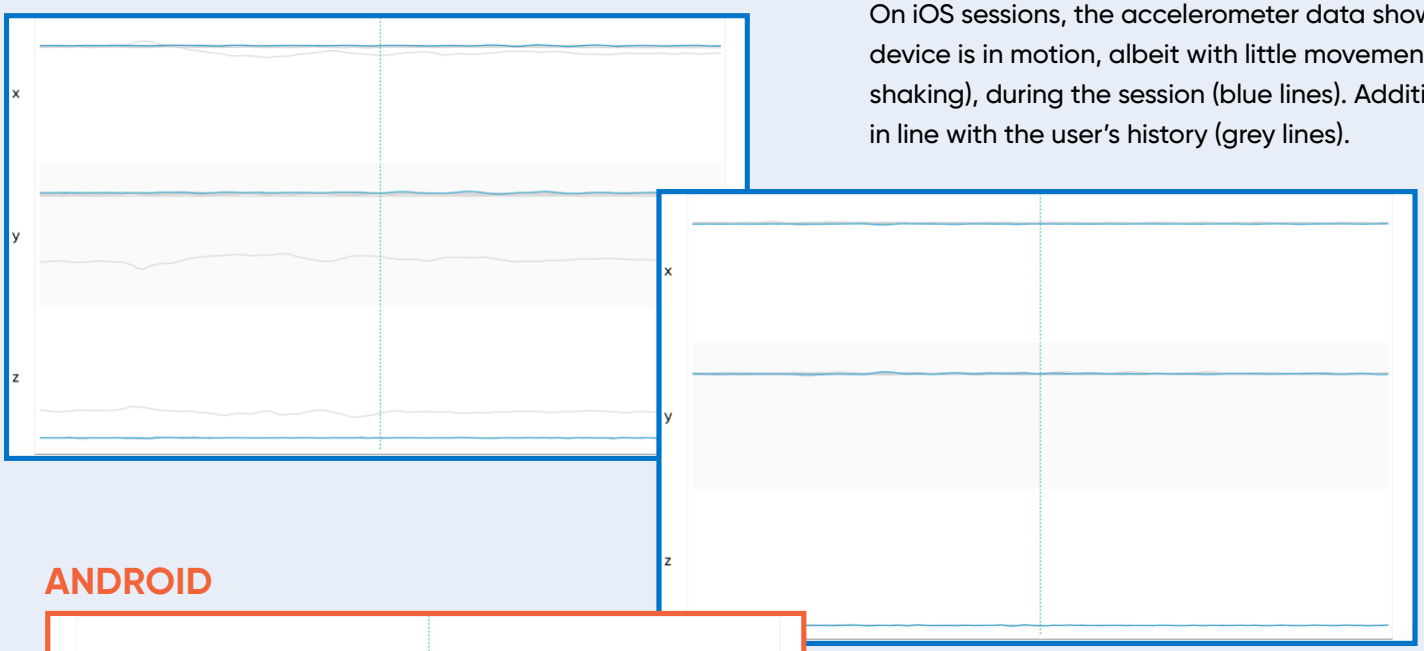
Activity in centre of screen – very uncommon for most users

Comparing the behaviour across the sessions, we see normal behaviour on iOS synonymous with standard mobile banking sessions, compared to non-human behaviours in the Android session. This difference lies in the session control – on Android, the session is controlled via RAT from a desktop computer – here we see active RAT – whereas on iOS such control is not possible, so the device owner is interacting directly – passive RAT.

ACTIVE/PASSIVE RAT:

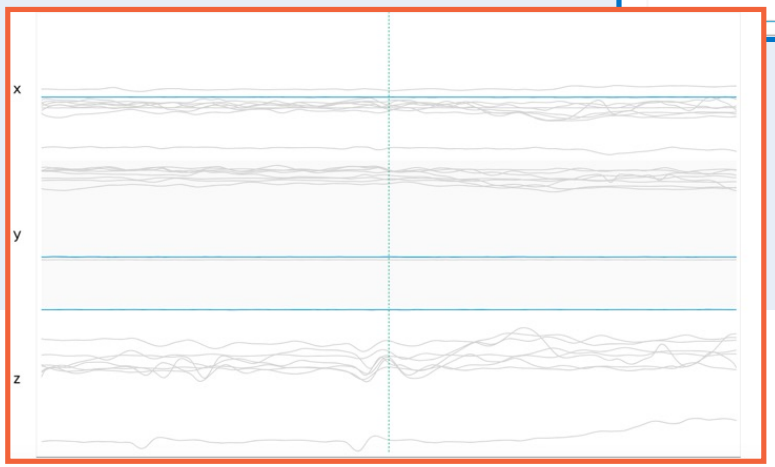
Accelerometer Data

iOS



On iOS sessions, the accelerometer data shows the device is in motion, albeit with little movement (most likely shaking), during the session (blue lines). Additionally, this is in line with the user's history (grey lines).

ANDROID



Android sessions show flat lines for fraudulent sessions, suggesting the device is potentially lying on a flat surface. In general, the movement does not align with user's history.

Once again, we see clear signs of remote access on the Android session, while the iOS sessions exhibit normal user behaviour.

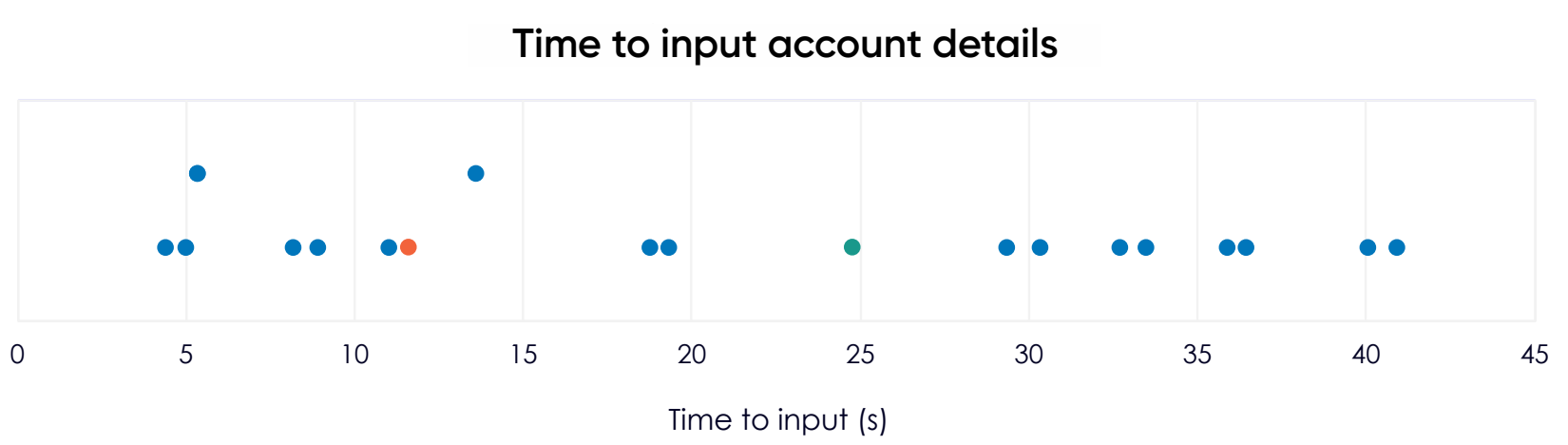
ACTIVE/PASSIVE RAT:

Time to Input Account Details

In Session #1, we see the user pastes information, which is readily available, and completes the fields within just 15 seconds.

Session #1 (Android)

Session #2 (iOS)



In Session #2, the user types the account details in blocks of two – a sign of dictation – and even corrects some information – something more prevalent in scam cases where information is not in the hands of the user. Ultimately, this results in the user taking almost 3 times as long to input the information.

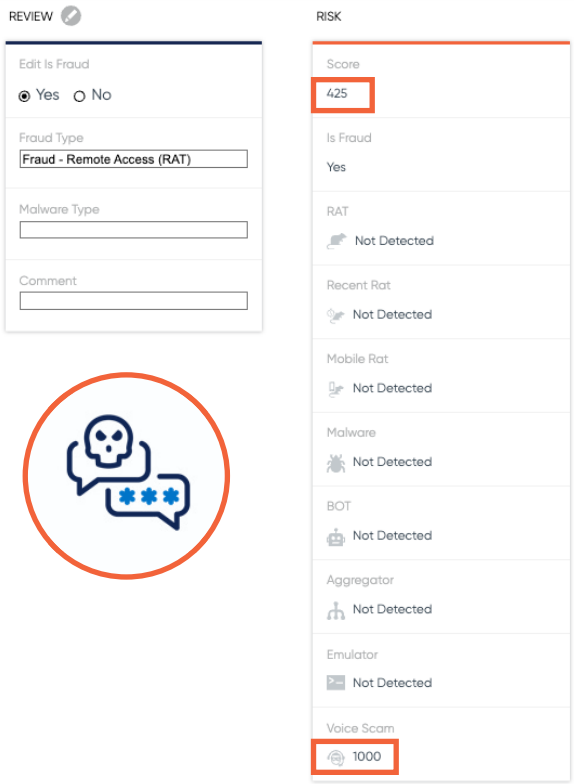
KEY Typed character · Deleted character · Click between fields

The interaction on the Android session is unusual, suggesting the user has the information readily available. Meanwhile, the iOS session, once again, shows normal user interaction.

ACTIVE/PASSIVE RAT:

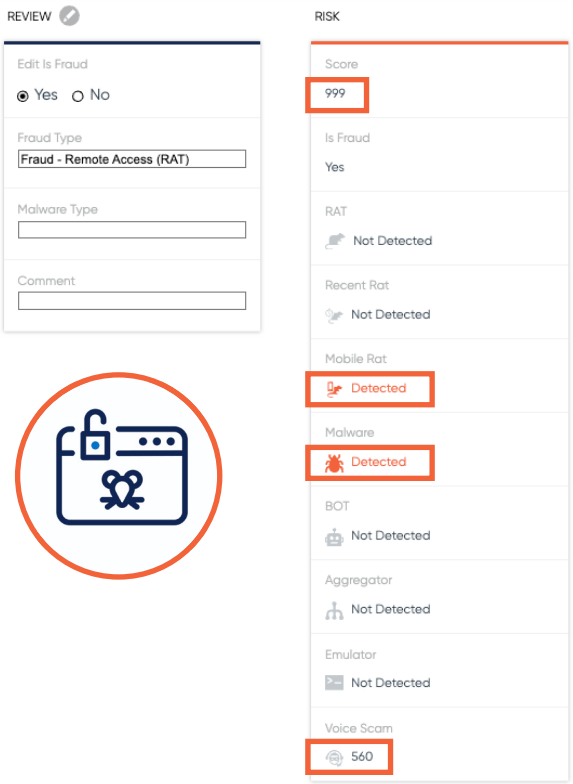
Account Takeover Model Outputs

iOS Session



The ATO score, which indicates the session may have been done by a third-party, is low; meanwhile, there is a high voice scam score, suggestion potentially coercion.

Android Session



There is a high ATO score, and a mid-range voice scam score. This would imply third-party control of the session. Additionally, we see threat indicators that show the use of RAT on a mobile device, as well as known malware behaviours (likely a malware strain that uses RAT).

In addition to the model scores, the model generates a series of risk and genuine factors, which have been analysed separately.

At the genuine factors level, we see consistency with the user profile history, suggesting that these sessions (from both platforms) took place on the victims' devices.

However, it is when we analyse the risk factors where we see indicators that suggest the behaviour is different across iOS and Android. The iOS session shows a risk factor indicating screen broadcasting took place, with no other significant behavioural risks present in the session. Meanwhile, the Android session provides a total of 10 risk factors that are consistent with third-party control via remote access tools.

ACTIVE/PASSIVE RAT:

Looking at the Data

The cases shown provide an interesting look at how behaviour can lead us to question the initial categorisation of a fraud case.

Looking at regional data in this regard, we see that 63% of all remote access sessions from an iOS device showed indications of potential coercion, as per our voice scam model. 74% of these sessions resulted in high scores often leveraged by banks. In comparison, on Android devices, only 42% showed such signs, dropping to 37% on web devices.

While it is easy to assume a categorisation based off the mention of TeamViewer or other remote access tools, we must remain watchful and work to understand the modus operandi at hand. As seen, the use of remote access tools can also be to watch and use this to prompt victims into how to continue with the impersonation scams. We can call this use of remote access 'passive RAT', where it is activated but not playing an important part in the execution of the session, and therefore not influencing the behavioural data available.

iOS Session

63% of all remote access sessions from an iOS device showed indications of potential coercion.

74% of these sessions resulted in high scores often leveraged by banks.

Android Session

42% of all remote access sessions from an Android device showed indications of potential coercion

37% of these sessions resulted in high scores often leveraged by banks.

ABOUT BIOCATCH

BioCatch stands at the forefront of digital fraud detection, pioneering behavioral biometric intelligence grounded in advanced cognitive science and machine learning. BioCatch analyzes thousands of user digital interactions to support a digital banking environment where identity, trust, and ease coexist. Today, more than 25 of the world's leading 100 banks and >100 of the largest 500 rely on BioCatch's solutions to combat fraud, facilitate digital transformation, and grow customer relationships. BioCatch's Client Innovation Board, an industry-led initiative featuring American Express, Barclays, Citi Ventures, HSBC, and National Australia Bank, collaborates to pioneer creative and innovative ways to leverage customer relationships for fraud prevention. With more than a decade of data analysis, over 80 registered patents, and unmatched expertise, BioCatch continues to lead innovation to address future challenges. For more information, please visit www.biocatch.com.

BioCatch