2024

Global Fraud & Scams Trends Report

AI-Powered Scams, Malware-as-a-Service, and Faster Payment Threats

OUTSEER

Table of Contents

Introduction

The skyrocketing popularity and widespread availability of AI in the past year has fueled an alarming surge in scams. Additionally, the increase in consumer accessibility to instant payments has led to a resurgence in instant payment scams and increasing reliance on money mules. These phenomena can be attributed to fraudsters' perpetual quest to enhance the efficiency of their scams and expedite the cash-out process by capitalizing on emerging technologies and consumer behavior shifts.

As financial crime escalates annually, companies must remain abreast of the latest trends and adapt their strategies to combat constantly evolving fraud tactics.

The Outseer Global Fraud and Scams Trends Report offers a comprehensive analysis of fraud attacks and consumer fraud data collected and analyzed by our team of fraud experts. Leveraging our proprietary insights gained from safeguarding Outseer customers, this report sheds light on the ever-evolving cyber fraud landscape that affects organizations of all sizes.

Fraud Threats & Trends

While the fraud landscape, from phishing to malware and brand abuse, remains consistent year after year, fraudsters persistently refine their techniques; prompting the evolution of fraud threats and corresponding mitigation strategies shaped by current events and technological advances.

Outseer sought out to address pressing questions:

What trends have exerted the most significant influence on fraud threats and mitigation over the past year?

What nuances require more attention?

In the pursuit of answers, we analyzed our own internal data in the context of current technology and shifts in fraudster behavior. This has surfaced what we believe to be the top three primary fraud threats, which we address in the report:

1. AI-Powered Scams
2. Malware-as-a-Service
3. Faster Payment Threats

Methodology

This report is based on the analysis of data generated from the Outseer Fraud Action 24/7 Anti-Fraud Command Center, established in 2004. With 20 years of data gathered from hundreds of clients worldwide, we have gained unique insights into the continuously evolving fraud trends.

200M+
URLs checked per month

200K+
attacks shutdown per year

5.5M+
compromised credit cards detected per year

15M+
compromised emails detected per month

Outseer's Anti-Fraud Command Center utilizes machine learning algorithms to monitor brand abuse and identify rogue attacks. The algorithms detect anomalies and signals indicative of fraudulent URLs and compromised credit cards and emails. Upon detection, our team of cybersecurity intelligence experts conducts forensic analysis to examine and authenticate potential threats, ultimately resulting in the generation of detailed intelligence.

Executive Summary

Key findings from the report include:

1

Trojan attacks experienced the largest year-over-year increase in attack volumes, driven by refined phishing tactics.

The rise of Malware-as-a-Service emerged as a significant cybersecurity threat as the volume of malware events surged 120% in the total volume of attacks year-over-year, compared to a 5.5% increase in phishing attacks and a 25% and 7.7% *decrease* for rogue mobile app attacks and brand abuse attacks, respectively. Malware-as-a-Service enables any fraudster with $50–200 dollars to evolve into a complex cyber threat that uses malware to enable their fraud attacks.

Polymorphic malware is not a new concept, but fraudsters are now using generative AI to reduce the skill level required to spawn malware variants that elude signature-based security systems, consequently challenging the efficacy of existing security protocols. This has been seen increasingly in banking Trojans, which intercept notifications and bypass alerts requiring secure channels. And their persistence easily evades detection on mobile devices.

2

The increase in mobile banking and Malware-as-a-Service have sent malware attacks to all-time highs.

The role of malware in fraud was a major theme through 2023. Fraudsters have taken an interest in information-stealing malware, Malware-as-a-Service and other 'as-a-service' type offerings, so much so that while the volume of fraud observed grew 108%, malware attacks grew by a staggering 4,000% or 40X growth in volume, partially due to the increase in malware in mobile channels. Part of this can be attributed to the rise in mobile app usage. With the increased usage, fraudsters are targeting the channel.

3

The adoption of real-time payments has increased APP scams; some countries are responding with regulation and liability shifts.

Outseer has seen a significant uptick in unauthorized push payments, mule accounts, and account takeovers in markets where faster payment adoption is high. Surveyed financial institutions saw a spike in fraud attacks using real-time rail: 57% reported mule activity was up, 71% reported consumer ATO had increased, and 62% reported APP fraud had increased.

The UK and EU have been on the forefront of change with the introduction of the Payment Systems Regulator (PSR) and the upcoming Payment Services Directive 3 (PSD3). In late 2024, the specifics of PSD3 and the implementation of the PSR liability shift will be revealed.

4

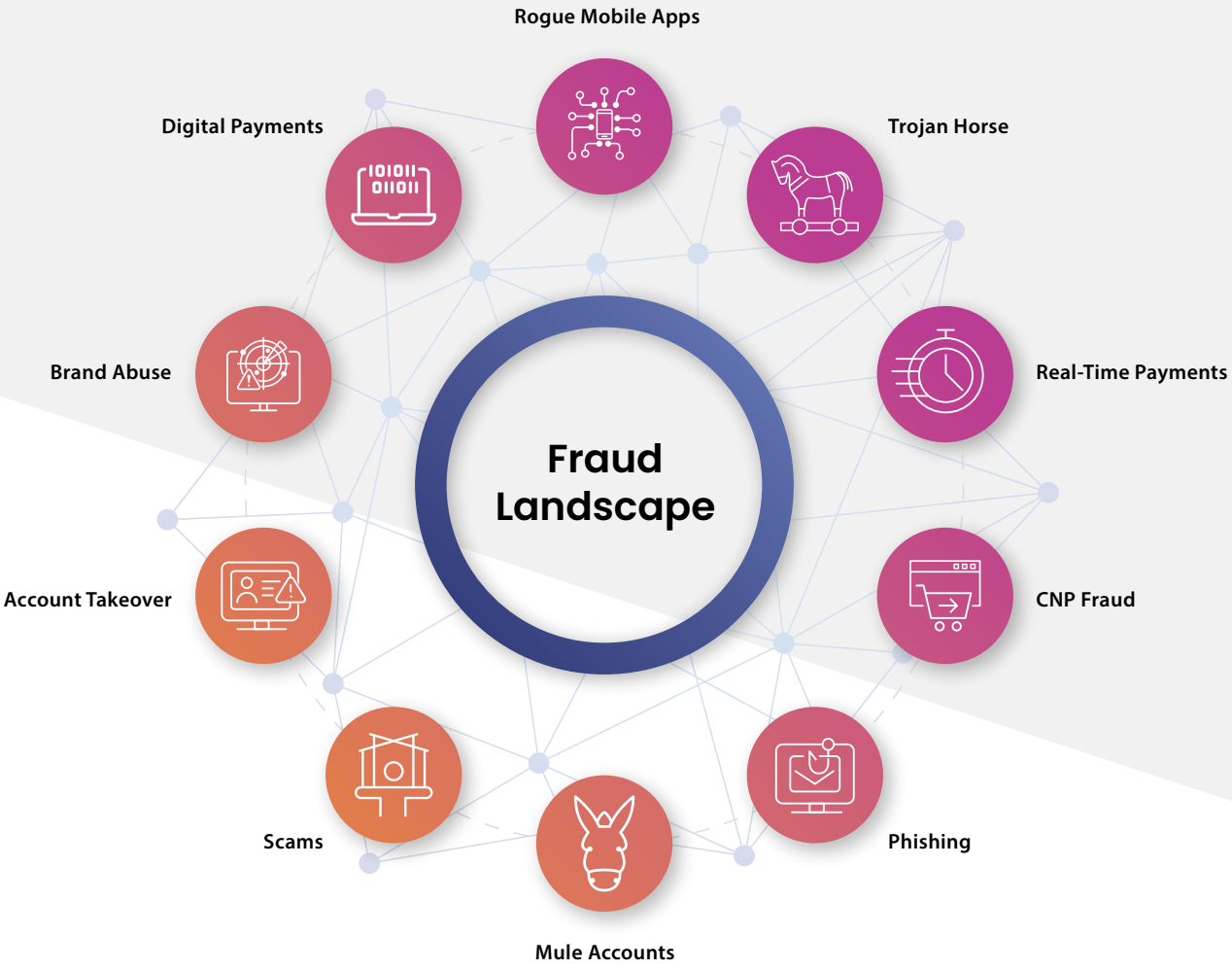
Prediction: The rise in AI will fuel scams and corresponding losses in the coming year.

AI has dominated the headlines over the past year and fraudsters have already begun to exploit this technology, with several major scams reported globally. With new AI tools and technology at their disposal, fraudsters are creating varied phishing emails that defeat existing scam and spam email filters. In addition to improving tried-and-true techniques, fraudsters are using AI more often on deepfakes, voice cloning, verification fraud, and authorized push payment (APP) fraud.

While Outseer didn't see direct fraud losses from generative AI in 2023, we predict that the scams and corresponding losses will continue to grow. Given the goal of generative AI scams is to trick people into believing what fraudsters put out there, Outseer does believe that generative AI contributed to the increased effectiveness of phishing tactics that fueled an even larger increase in Trojan attacks and malware attacks.

Despite the ways generative AI is being manipulated, predictive AI has also played a pivotal role in detecting cyber threats such as brand abuse, phishing, Trojans, and rogue mobile apps. The strength of AI and machine learning in combating these threats lies in their ability to continuously learn, adapt, and detect evolving patterns of malicious behavior across various digital landscapes. These technologies enable proactive and adaptive security measures, ultimately contributing to a more robust defense against cyber threats.

The Fraud Threat Landscape



Here is a summary of the types of common attacks that Outseer sees year-over-year:

Brand Abuse

Brand Abuse,[1] also called "brand exploitation" or "brandjacking", enables opportunists to capitalize on the shift to digital by impersonating your brand through fake sites, mobile apps, and social media pages. With the shift to digital, this form of fraud remains the most common.

Phishing

Phishing[2] is a form of cyberattack attempting to steal personal information from unwitting end-users under false pretenses, either by email, phone (vishing), or SMS text (smishing). The attackers trick users into believing they are involved with the company they are impersonating so they can get user credentials.

Rogue Mobile Apps

Rogue apps[3] are mobile applications designed to impersonate trusted brands with the goal of gaining unauthorized access to information used to commit fraudulent transactions. These malicious apps can install malware, ransomware, or trick users into sending their payment details to attackers. They don't necessarily fit the definition of malware since they don't take control of your device. However, they are extremely effective in fraud schemes. In a recent study, apps collected upwards of $38 million in revenue due to fees from fake apps that were cloned from real apps.

Trojan Horse

Trojan Horses are stealthy malware installed under false pretenses, attempting to steal personal user information.

2023 Global Fraud Trends

Outseer's analysis of global fraud trends across various attack vectors in 2023 reveals the year-over-year changes in the overall volume of attacks.

While phishing saw a moderate attack increase, brand abuse and rogue mobile app attacks saw a decrease in volume. However, Trojan horse attacks saw sizeable increases in the volume of attacks.

9%

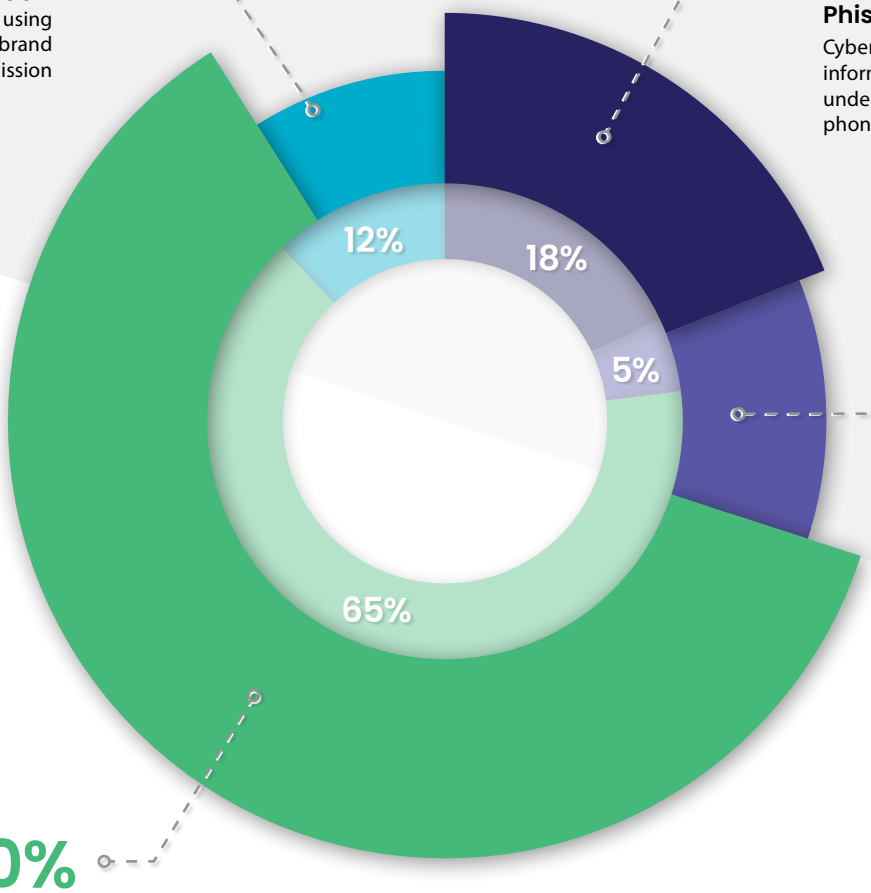
Rogue Mobile Apps

Mobile applications using an organization's brand without permission

19%

Phishing

Cyberattacks attempting to steal personal information from unwitting end-users under false pretenses—either be email, phone call (vishing), or SMS text (smishing)



11%

Trojan Horse

Stealthy malware installed under false pretenses, attempting to steal personal user information

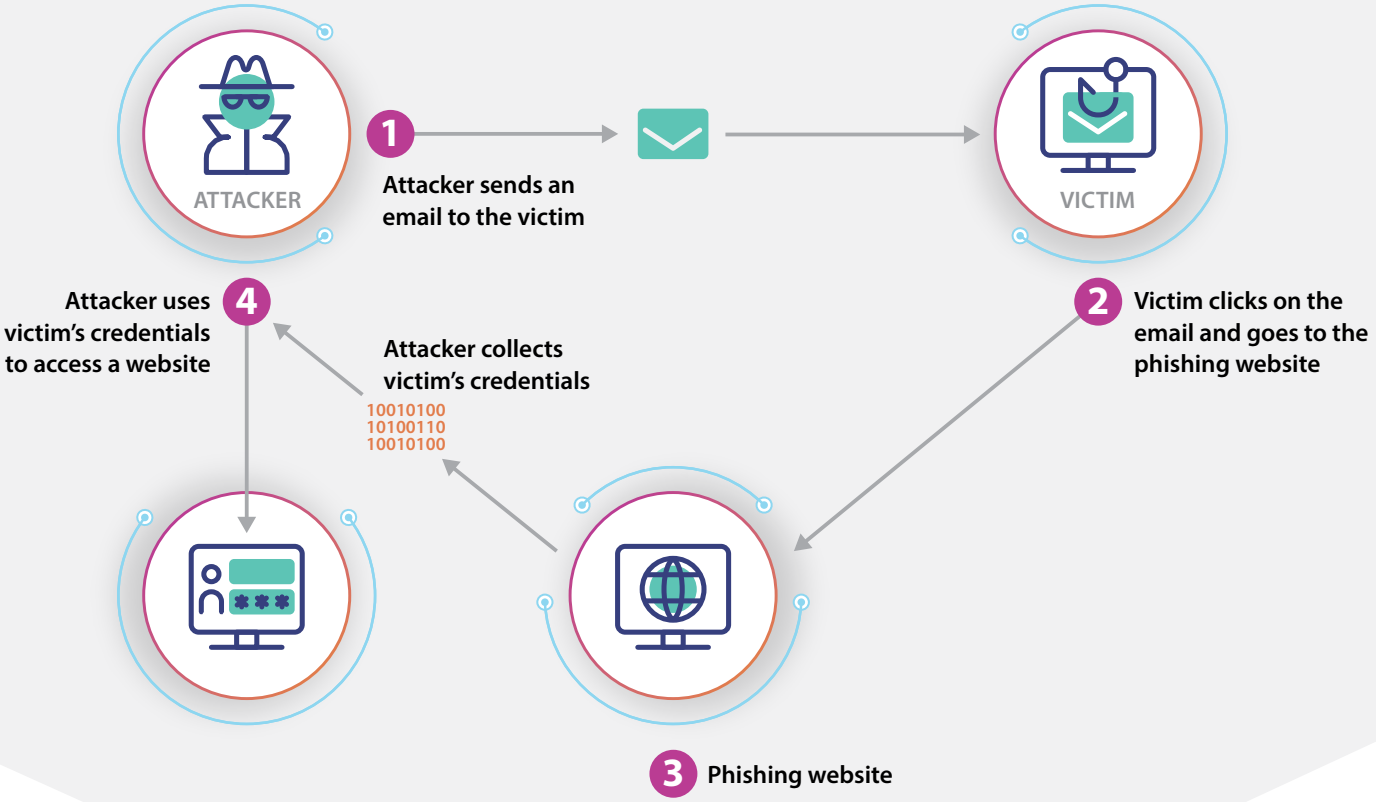
60%

Brand Abuse

Online content (e.g., social media) that misuses an organizations's brand with the purpose of misleading users

2023 vs 2022

Global Hosted Phishing Ecosystem



Fraud attacks continue to pose a significant threat to individuals and organizations worldwide. Phishing is notable because it is the entryway for many other attacks and scams. It is also very difficult to track, and more importantly, difficult to take down fraud rings.

Cybercriminals strategically exploit servers across different regions to carry out their malicious activities. While specific regions are notorious for hosting these malevolent servers, cybercrime transcends borders and attacks can originate from servers located in any country.

Trend #1: AI-Powered Scams

The Role of Generative AI for Fraud & Predictive AI for Fraud Prevention

AI has dominated the headlines over the past year, sparking numerous discussions and debates over its merits and potential downfalls. Within fraud prevention, AI assumes a dual role, serving as both an empowering tool for fraudsters and a defense mechanism for those combating fraudulent activities. Fraudsters consistently demonstrate agility in exploiting emerging technologies. The rapid adoption of advancements, such as generative adversarial network (GAN) models,[4] coupled with the exponential growth of data, fraudsters have the means to refine their tactics, crafting increasingly sophisticated cyber threats that evade traditional detection systems.

The proliferation of generative AI and its ability to generate remarkably realistic content and scenarios has contributed to the escalation of authorized fraud. For example, earlier this year, a Hong Kong finance employee thought he received a message from the company's UK-based chief financial officer asking for a $25.6 million transfer.[5] Though initially suspicious that it could be a phishing email, after a deepfake video call with the CFO and other colleagues he thought the request was legitimate. It was only after reaching back out to the head office that he discovered that it was, in fact, a scam. Unfortunately, by then the money was transferred.

In another example, over 50 deepfake videos were posted of well-known celebrities,[6] encouraging people to invest in a non-existent cryptocurrency platform seemingly promoted by Elon Musk. While it is unknown how much was lost in this instance, the videos had tens of thousands of views when removed.

While Outseer didn't see direct fraud losses from generative AI scams in 2023, we predict that the scams and corresponding losses will continue to grow. Given the goal of generative AI scams is to trick people into believing what fraudsters put out there, Outseer does believe that generative AI contributed to the increased effectiveness of phishing tactics that fueled an even larger increase in Trojan attacks and malware attacks.

While generative AI poses significant challenges, the deployment of predictive AI and machine learning has emerged as a crucial countermeasure in identifying and taking down fraudulent schemes including brand abuse, phishing attacks, Trojans, and rogue mobile apps.

Generative adversarial networks can create deep fakes by using large datasets to generate new content similar to the original.

Scams Using AI

Phishing

5.5%
increase
19% of overall attacks
(Second largest in volume)

In the past year, Outseer saw an increase in volume of 5.5%, going from 18% of attacks identified to 19% of attacks. During this time frame, there was a short-term spike in Q2 and Q3 2023 before decreasing slightly in Q4. Trojan and malware attacks have been the driving force behind this trend. Though they are not new, they continue to remain popular, as they are effective and are often the entry point to other scams.

With AI tools such as ChatGPT, fraudsters are creating improved phishing emails that can instantly create bodies of text that impersonate the tone and coherence of legitimate messages, for free. Misspellings, clumsy grammar, and other tell-tale signs of a fake email can be added or removed on-demand depending on need. More concerning is the ability to use large language models to rephrase dozens to hundreds of email variants. Spam and scam email filters are a major tool used to stop fraud, but they rely on filtering identical or highly similar emails flagged as scams and spam. With the ability to use automation and AI to generate so many variants of the same phishing campaign, these filters are significantly undermined. This type of software is freely available, and although ChatGPT has some built-in functions to stop it from being misused, these can be easily subverted. These emails are now slipping through conventional security measures and fooling more users into providing their credentials.

Brand Abuse

7%
decrease
60% of overall attacks
(Largest in volume)

Fraudsters have been successful in replicating brand logos and websites for unsuspecting users to land on through their phishing emails and other measures for years, fooling users into providing credentials to collect money.

When looking across all attack vectors, brand abuse remains the most prevalent at 60% of all detected attacks. However, overall, brand abuse has decreased on a quarter-on-quarter basis in the past two years after peaking in early 2022, for a total decrease of 7%. At the peak in Q1 2022, brand abuse accounted for 81% of observed attacks. It decreased to 65% in 2022, and to 60% in 2023.

Trojans & Rogue Apps

Fraudsters are using generative AI to lower the technical skill level needed to produce malware variants that elude signature-based security systems; therefore, challenging the efficacy of existing security protocols. This has been seen increasingly in banking Trojans, which intercept notifications and bypass alerts requiring secure channels. And, they are persistent, easily evading detection on mobile devices.

AI and machine learning play a dual role in Trojans:

- **Detect:** AI is used to detect and prevent fraudulent activities. AI algorithms do this by analyzing patterns, anomalies, and user behavior to identify rogue apps and Trojans.
- **Create:** AI is used by fraudsters to create more convincing rogue apps. AI can generate realistic interfaces, simulate user interactions, and adapt to security measures.

Outseer saw a 120% increase in Trojans this past year, discussed more in depth with respect to Malware-as-a-Service.

120%
increase in Trojans

Hydra

Octo

Alien

Hook

A 5.5% spike in phishing led to a 120% increase in Trojan and malware attacks.

AI Fueling Scam Growth

Deepfakes

In the past few years, fraudsters have harnessed deepfake technology with remarkable success. This cutting-edge technique allows them to quickly create convincing audio and video content, meticulously mimicking the voices and appearances of trusted individuals, including celebrities or even CEOs.

Leveraging machine learning, fraudsters can rapidly and inexpensively train neural networks using footage of their targets. As a result, they achieve uncanny accuracy in replicating not only the person's voice but also subtle nuances like inflection and tone. The integration of artificial intelligence further enhances the realism of the generated voice and video.

The implications are concerning: these fabricated personas can propagate falsehoods, manipulate unsuspecting victims, and orchestrate fraudulent schemes. For instance, they might coerce individuals into transferring substantial sums of money or exploit the trust inherent in relationships with the impersonated individual.

Voice Cloning

Voice cloning with artificial intelligence can accurately reproduce an individual's tone and language. This technology is employed to create the illusion of authentic phone conversations with trusted parties.

One such example is "grandparent scams" where the voices of either the grandparent or grandchild are replicated.[7] By fabricating scenarios like accidents, voice cloning becomes a successful tool for extorting money from unsuspecting loved ones. We also expect to see this increase given the increasing usage of online banking and call centers.

Verification Fraud

Numerous verification methods exist for sensitive phone or bank information. Unfortunately, these methods are susceptible to exploitation. Recently, voice verification has become a more frequent target for fraud, with AI technology being employed to undermine security checks. This poses a significant risk for both consumers and financial institutions. Once a perpetrator records a sample of a victim's voice, they can exploit it to bypass voice verification mechanisms using AI-generated content.

Authorized Push Payment Fraud

AI is increasingly used in Authorized Push Payment (APP) Fraud,[8] which includes impersonation scams, purchase scams, romance scams, and more where the end goal is getting the victim to execute an instant payment. Its effectiveness lies in the ability to manipulate people to get them to willingly transfer their money. With instant payments, recovery of those funds after transfer through a network of mule accounts is extremely difficult.

Scams Expected to Increase

1. Deepfakes
2. Voice Cloning
3. Verification Fraud
4. Authorized Push Payment Fraud

Recent Developments in Generative AI

OpenAI's recent announcement of Sora, an AI capable of generating hyper-realistic videos and imaginative scenes from simple text prompts or sample images, marks a significant advancement in technology. This innovation could potentially empower scammers by providing them with unparalleled capabilities to make their fraud that much more realistic in order to gain substantial profits. With the ability to produce convincing celebrity deepfakes, perpetuate misinformation, craft realistic romance scam videos, and orchestrate crypto scam advertisements or spear-phishing campaigns aimed at unsuspecting employees and consumers, Sora raises concerns about the misuse of such powerful software.

Recognizing the potential for fraud, OpenAI pledged to vet Sora before its release. However, despite its promising capabilities, the ethical implications and risks of misuse remain. This is a development that we will closely monitor as we progress into 2024 and urge other organizations and consumers to do the same.

"Beyond Our Reality" (Sora & Donald Allen Stevenson III)

AI for Good

Despite the ways generative AI is being manipulated, AI—especially predictive AI (machine learning)—has also been a force for good by playing a pivotal role in detecting cyber threats such as brand abuse, phishing, Trojans, and rogue mobile apps. The strength of AI and machine learning in combating these threats lies in their ability to continuously learn, adapt, and detect evolving patterns of malicious behavior across various digital landscapes. These technologies enable proactive and adaptive security measures, ultimately contributing to a more robust defense against cyber threats.

Brand Abuse Detection

Machine learning enables the analysis of vast amounts of online data to identify patterns associated with brand abuse. It can recognize unauthorized usage of trademarks, logos, or other brand elements across different platforms. Machine learning models can continuously learn from new instances of abuse, adapting, and improving detection accuracy over time.

Phishing Detection

Machine learning employs sophisticated algorithms to analyze email content, URLs, and sender behavior to identify potential phishing attempts. Machine learning models can recognize patterns in email structures, language usage, and malicious links to distinguish phishing emails from legitimate ones. They learn from historical phishing attempts to enhance accuracy in detecting new threats.

Trojan Detection

Machine learning algorithms can detect Trojans by analyzing code behavior and characteristics. They can identify anomalies in software behavior that indicate potential Trojan activity. By learning from known Trojan patterns and behaviors, these models can continuously evolve to spot new variations.

Rogue Mobile Apps Detection

Machine learning-powered systems can scan app marketplaces for rogue mobile applications by examining app behavior, permissions, and developer details. Machine learning algorithms can identify suspicious activity or coding patterns indicative of malicious intent, thereby helping prevent the installation of harmful apps.

Trend #2: Malware-as-a-Service

The role of malware in fraud has been a major theme through 2023. Fraudsters have taken an interest in information-stealing malware, Malware-as-a-Service and other 'as-a-service' type offerings.

Increase in Malware Attacks

4,000% Malware attacks grew a staggering 4,000%

While the volume of fraud observed grew 108%, malware attacks grew by a staggering 4,000% or 40X growth in volume, partially due to the increase in malware in mobile channels. From Q3 to Q4 of 2023, malware was up 41% in a single quarter—all on top of already historic growth over the past two years. We predict that malware will continue its role as a significant factor in fraud prevention strategies going forward for banks and financial institutions.

Decline in Rogue Mobile Apps

While there has been an increase in malware attacks through legitimate mobile banking apps, attacks through rogue mobile apps, which emulate legitimate brand apps, have decreased by 25% since 2022, continuing a declining trend after experiencing a surge during the pandemic. The year-over-year percentage of total attacks decreased from 39% in 2021 to 12% in 2022 to 9% in 2023.

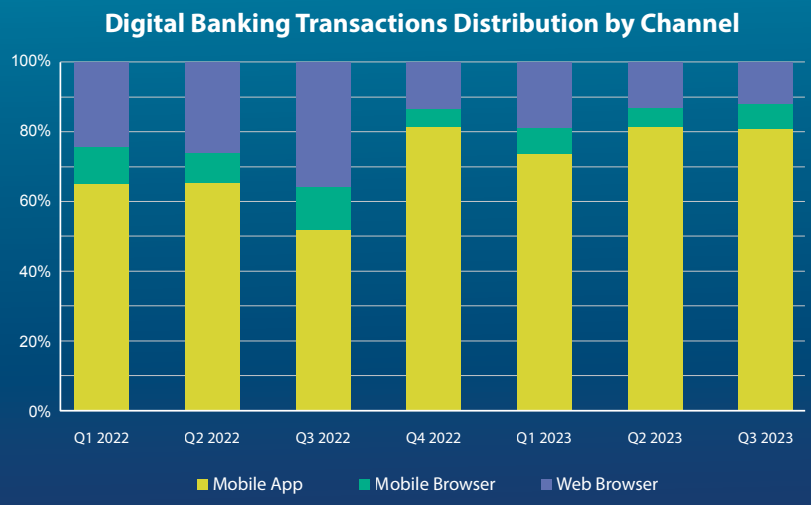
39% Decline in rogue mobile attacks

When customers increased their adoption of online and mobile banking, fraudsters began distributing rogue and malicious mobile apps to steal logins with the hope of stealing the money sitting in those bank accounts. However, maintaining and supporting these apps was more of a drain on resources and profits and fraudsters instead opted to scale up social engineering via brand abuse attacks—particularly on social media.

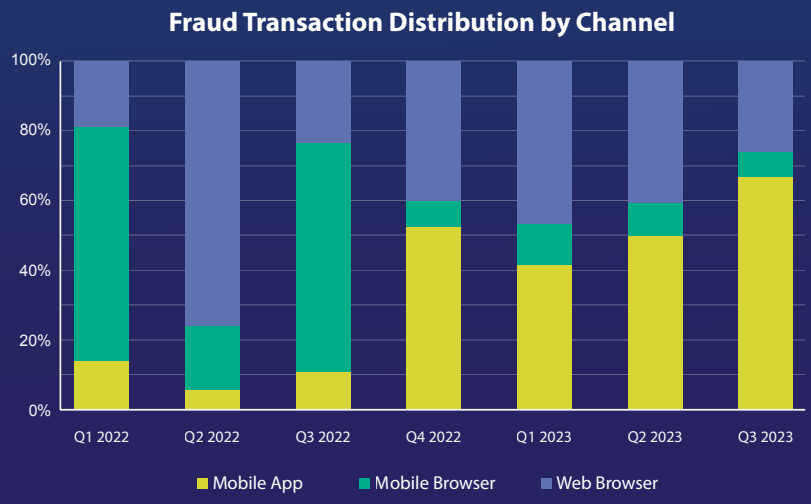
A Rise in Digital Banking Fuels Attacks Through Mobile

Mobile app usage continues to increase, and now comprises 85% in total traffic. Outseer has seen that the increase in this channel was accompanied by a parallel trend in increased mobile fraud, with 62% of detected fraud originating from mobile apps. This underscores the urgent need for implementing tailored and robust security measures to effectively address the escalating threat landscape within the mobile domain.

Increase in mobile app usage



Increase in mobile fraud



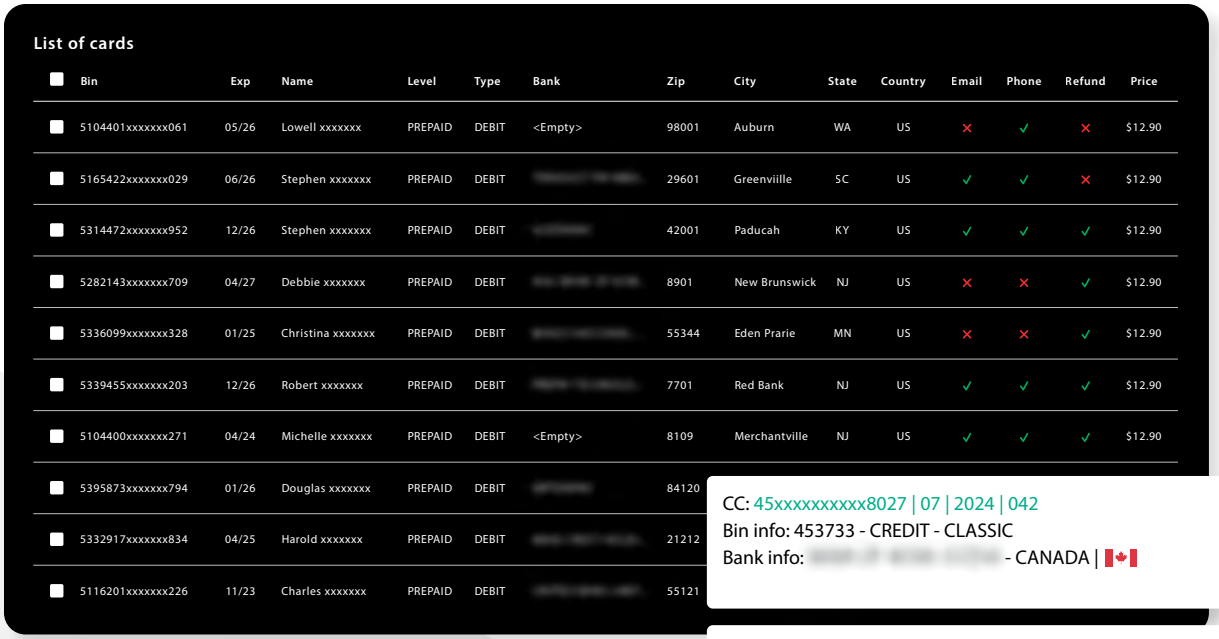
An increase in malware attacks is problematic at financial institutions even if there are no monetary fraud losses because operational expenses increase with customer-reported fraud. The expense of securing customer accounts lost to phishing or card numbers captured by fraudsters can easily run $30–$100 per customer impacted. This can translate into millions of dollars in operational losses spent, even before considering reimbursements to replace money lost to fraudsters and scammers. Costs associated with opening and closing new bank and credit card accounts also increase.

31.5M+

Outseer successfully recovered over 31.5 million compromised cards and card previews

Compromised Cards

In 2023, 31.5 million+ compromised cards and card previews were recovered. Data packets being sold on the dark web include compromised card information resulting from cyberattacks targeting online transactions and e-commerce platforms.



List of cards

Bin	Exp	Name	Level	Type	Bank	Zip	City	State	Country	Email	Phone	Refund	Price
5104401xxxxxxx061	05/26	Lowell xxxxxxx	PREPAID	DEBIT	<Empty>	98001	Auburn	WA	US	✗	✓	✗	$12.90
5165422xxxxxxx029	06/26	Stephen xxxxxxx	PREPAID	DEBIT	[redacted]	29601	Greenviille	SC	US	✓	✓	✗	$12.90
5314472xxxxxxx952	12/26	Stephen xxxxxxx	PREPAID	DEBIT	[redacted]	42001	Paducah	KY	US	✓	✓	✓	$12.90
5282143xxxxxxx709	04/27	Debbie xxxxxxx	PREPAID	DEBIT	[redacted]	8901	New Brunswick	NJ	US	✗	✗	✓	$12.90
5336099xxxxxxx328	01/25	Christina xxxxxxx	PREPAID	DEBIT	[redacted]	55344	Eden Prarie	MN	US	✗	✗	✓	$12.90
5339455xxxxxxx203	12/26	Robert xxxxxxx	PREPAID	DEBIT	[redacted]	7701	Red Bank	NJ	US	✓	✓	✓	$12.90
5104400xxxxxxx271	04/24	Michelle xxxxxxx	PREPAID	DEBIT	<Empty>	8109	Merchantville	NJ	US	✓	✓	✓	$12.90
5395873xxxxxxx794	01/26	Douglas xxxxxxx	PREPAID	DEBIT	[redacted]	84120							
5332917xxxxxxx834	04/25	Harold xxxxxxx	PREPAID	DEBIT	[redacted]	21212							
5116201xxxxxxx226	11/23	Charles xxxxxxx	PREPAID	DEBIT	[redacted]	55121							

CC: 45xxxxxxxxxx8027 | 07 | 2024 | 042
Bin info: 453733 - CREDIT - CLASSIC
Bank info: [redacted] - CANADA |
52 14:20

CC: 40xxxxxxxxxx5202 | 03 | 2026 | 361
Bin info: 405428 - DEBIT - CLASSIC
Bank info: [redacted] - UNITED STATES OF AMERICA |
49 14:20

CC: 49xxxxxxxxxx7173 | 02 | 2025 | 562
Bin info: 491566- DEBIT - ELECTRON
Bank info: [redacted] - MEXICO |
50 14:22

This compromised data is used in various fraudulent activities, including the unauthorized use of compromised cards, commonly referred to as “carding,” for purchasing goods both online and in physical stores. With fraudsters equipped with added technology and access to a larger pool of stolen data, their success rates have seen a significant rise.

Trojan Surge

The Persistent Rise of Android Banking Trojans

The rise of Android Banking Trojans emerged as a significant cybersecurity threat, surging 120% in the first half of 2023 alone. The percentage of total attacks increased from 5% to 11% year-over-year. Outseer believes it will continue to be a significant threat into 2024.

This surge has been largely driven by the proliferation of Malware-as-a-Service (MaaS).[9] These criminal software solutions enable non-technical fraudsters to use malware to steal customer information and passwords to later use in identity theft and account takeover attacks.

Command-and-Control Servers

A key aspect of Malware-as-a-Service is the use of decentralized Command-and-Control Servers (C&Cs or C2). The communication established between infected devices and these servers gives malware operators the ability to receive information on infected devices and execute additional commands remotely.

Malware families orchestrated under the Malware-as-a-Service model, including Hydra, Cerberus, and Octo. all resulted in notable surges in C&C infrastructure volumes.

Hook Android Banking Trojan

A direct descendant of the "Ermac" banking Trojan, designed to steal financial and personal information from mobile devices running the Android operating system, is the Hook Android banking Trojan. Armed with advanced capabilities, Hook encompasses contact harvesting, SMS interception, keylogging, 2FA interception, RAT capabilities, overlay injection, and more.

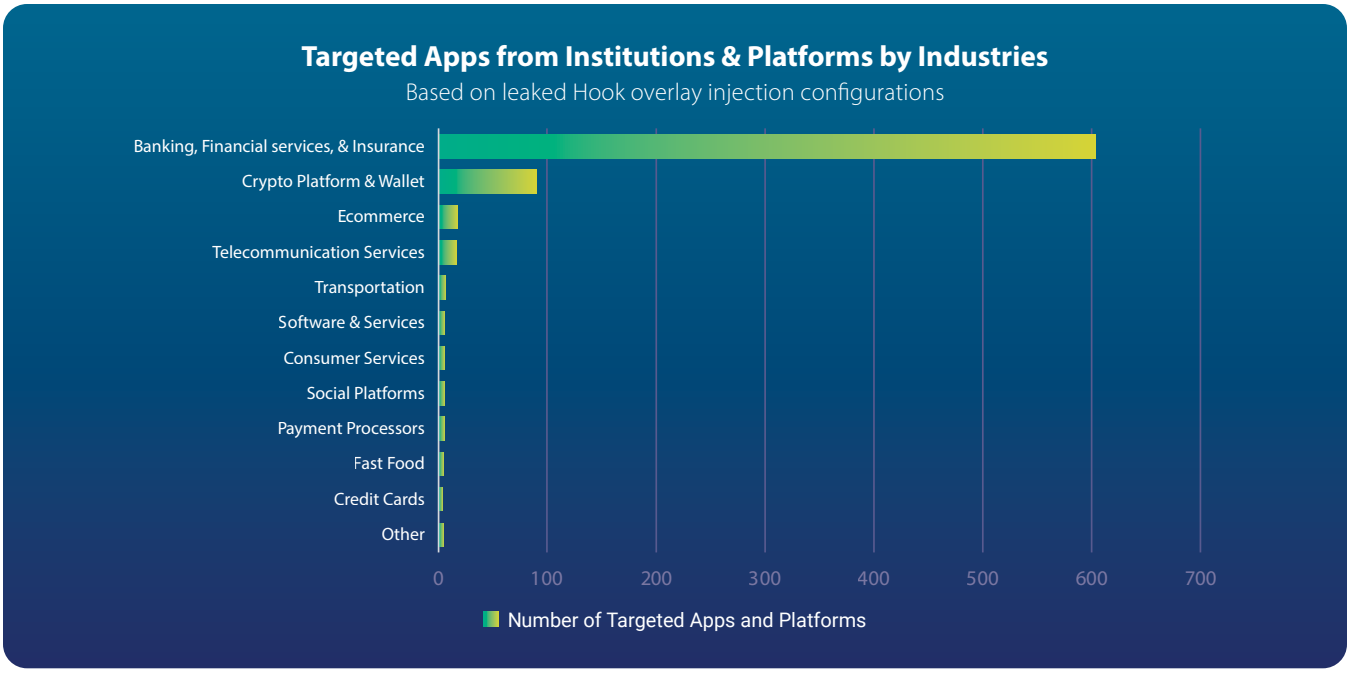
20% Hook leak contributed to the 20% surge in malware attacks

By design, Hook has over 750 injections at its disposal, where infected devices overlay a fake interface of a targeted brand—such as a financial institution's banking app—onto the legitimate app to deceive users into entering their sensitive financial information, targeting different brands worldwide. Moreover, the malware operator can add customized injections if desired.

A major event in the second half of 2023 was the leak of the Hook Android banking Trojan's APK and Panel source code using the C&Cs. Because of this leak, Hook garnered considerable attention and focus within the cybercriminal community. This newfound spotlight propelled Hook's contribution to the total number of C&Cs to be on par with the infamous Trojans Hydra, Cerberus, and Octo.

When threat actors identified the ability to easily profit, it led to the development and sale of customized overlay injections. They have now expanded attacks to target not only traditional financial institutions but also other financial sectors, including crypto wallets, streaming platforms, delivery services, and retail stores.

Command-and-Control Servers continue to serve as the central control hub for Android Banking Trojans, granting attackers remote control over infected devices. These servers are the operational core of the malware, enabling malicious activities.



Hook Signified a Turning Point for Fraud-as-a-Service

The introduction of new variants of the Android banking Trojan, such as Hook, signified a turning point in the mobile malware landscape with implications for future Trojan variants because it made it easy for fraudsters and fraud-as-a-service offerings to execute the banking Trojan or to develop new malware based on it. As with other Malware-as-a-Service offerings, it enabled even unsophisticated fraudsters to scale cyberattacks rapidly.

As fraudsters increasingly leverage Hook, we anticipate continuing to see new variants in the future, each with potentially enhanced functionalities and more dangerous capabilities. Given the threat Android banking Trojans pose, Malware-as-a-Service is far from concluded.

Outseer FraudAction Anti-Trojan Service (ATS) Team

The Outseer FraudAction ATS (Anti-Trojan Service) team continuously monitors C&Cs. For the first half-year of 2023, the number of active Hook C&C servers remained relatively low compared to other well-known banking Trojans. However, by the end of October 2023 (when the source code of Hook leaked), a significant surge in C&Cs associated with Hook was detected—making it one of the most active trends in the Android banking Trojans realm. This event led to massive growth in HookBot C&Cs, with over 200 new C&Cs detected in the last couple of months of 2023.

200+ Over 200 new C&Cs were detected in Q4 of 2023

The Importance of Monitoring & Takedown

Recent growth in phishing, scams, and malware has made it clear that relying only on controls handling anomaly payment detection or anomaly login detection is insufficient. Companies must be proactive in fraud prevention, fighting against brand abuse scams, phishing, and the spread of malware. Waiting to react until the fraudster has access to the account or until the money is moving could prove very costly.

Adopting a proactive defense to disrupt phishing and malware stops fraud before it needs to be mitigated by operations teams, netting a massive savings of 10-to-1 or more in reduced operational expenses at call centers and banking ops teams.

Monitoring & Takedown Through FraudAction

Outseer FraudAction helps companies proactively disrupt fraudulent activities, preempting harm to financial institutions, brands, and customers. Through continuous monitoring, we swiftly identify and dismantle phishing sites, malware, and social media brand abuse, while also fortifying defenses against business email compromise. Our cyber-intelligence service scours the dark web, equipping financial institutions with actionable threat intelligence reports and data feeds such as compromised credit cards and mule accounts for effective risk mitigation.

Trend #3

Faster Payment Threats

The Adoption of Faster Payments

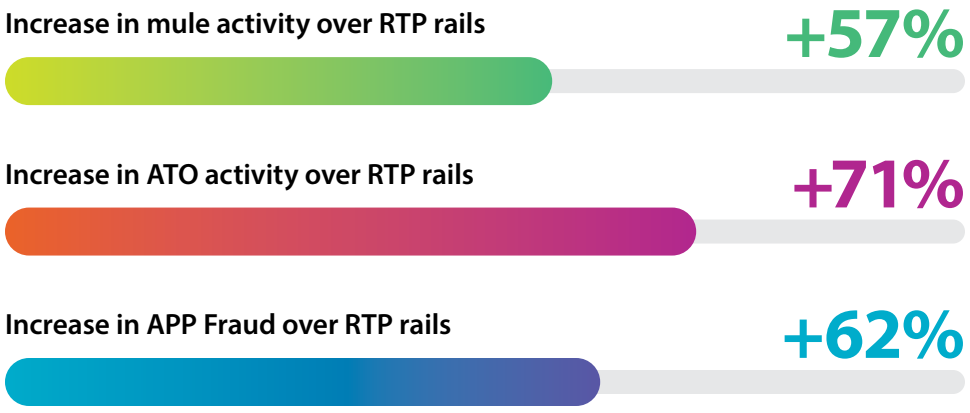
Faster payments—the electronic transfer of payments designed to speed up the process of sending money—have seen their adoption accelerate globally. The UK's Faster Payment Service launched in 2008, India's Unified Payments Interface (UPI) launched in 2016, Brazil's faster payments rail PIX launched in 2020, and the US saw the launch of Zelle and Real-Time Payments (RTP) in 2017 with FedNow in 2023.

Currently, more than 70 countries on six continents support real-time payments, representing 195 billion transactions in 2022 and a 63% year-on-year growth.[10] The countries with the highest volume of faster payment transactions were India, China, Thailand, and Brazil, with annual transactions ranging from 49 billion in India to 9 billion in Brazil.[11] However, the US RTP volume in 2023 was low at only about 249 million, and as of March 2024, only 5% of US financial institutions participated in US RTP or FedNow, showing that the US is still in the early phase of instant payments.

While the term "faster payments" is often used as an umbrella term for real-time and instant payments, they are all similar in that they are payments made between bank accounts that are initiated, cleared, and settled quickly at any time of the day or week. While the speed of these payments helps to improve convenience, transparency, and confidence in payments, it also increases the chances for fraud, and in particular authorized push payment (APP) fraud, when a fraudster tricks their victim into transferring funds into their account by pretending to be a legitimate payee. In many cases, this happens via social engineering across social media networks, or by phone. In many markets, APP fraud is growing faster than card fraud.

Faster Payments, Faster Fraud

Over the past few years, Outseer has seen a significant uptick in unauthorized push payments, mule accounts, and account takeovers in markets where faster payment adoption is high.



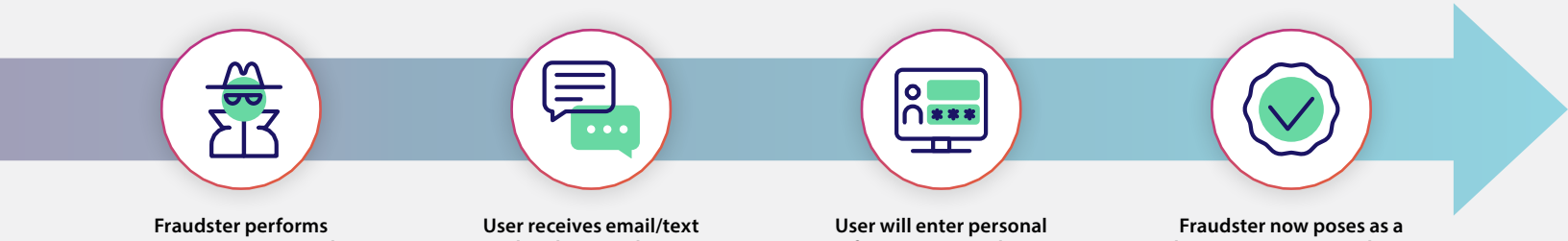
In a recent survey,[12] the majority of financial institutions saw a spike in fraud attacks using real-time rail: 57% said mule activity was up, 71% said consumer ATO had increased, and 62% said APP fraud had increased. This has translated into real dollar losses as well. For example, in the UK, APP scams were reported to be £485 million ($618 million in U.S. dollars), which accounts for 40% of U.K. bank fraud losses.[13] Experts predict these crimes could cost $4.6 billion in the U.K. alone by 2026.[14] The U.S. Federal Trade Commission (FTC) estimates that scams in the U.S. cost consumers $8.8 billion in 2022, an increase of approximately 30% from 2021.[15]

The majority of financial institutions have seen an increase in fraud attacks when using real-time payment rails.

With the introduction of FEDNOW in the US and the increasing adoption of instant payment systems across the globe, combined with the success fraudsters are seeing in these types of scams, more opportunities for scams are expected.

Stopping these scams is difficult because the victims authorize the transactions, often without the realization they are a scam target until after the payment clears.

How Do These Scams Work?



Fraudster performs reconnaissance attack to gain customers information

User receives email/text with either attachment or link containing malware or phishing website

User will enter personal information or malware will steal sensitive data

Fraudster now poses as a legitimate person and can use data to build trust and perform an account transfer

Scams rely on the fraudster knowing personal information about customers. In order to gain this information, fraudsters often execute a phishing attack or buy/obtain the information from elicit sources such as the dark web. Once the fraudster has obtained personal information about the potential victim, it becomes easier for them to forge connections, enhancing their credibility.

For example, a fraudster who calls a customer by their first name and confirms their banking institution or other personal information will always seem more genuine than a cold call where the fraudster has no connection with the customer.

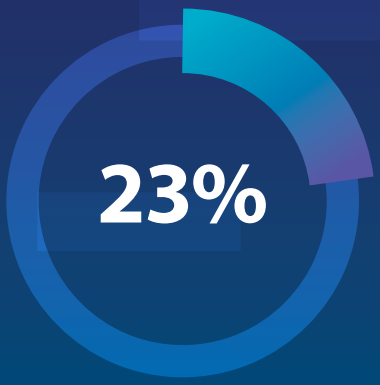
The consumer is the weakest link in this process because fraudsters have developed and perfected a playbook and have replicated this attack vector across multiple geographies. The challenges with stopping fraudsters from obtaining such personal information rely heavily on customer education regarding potential threats since there is no easy way to detect authorized fraud where the consumer is "tricked."

Money Mule Contribution to Faster Payments

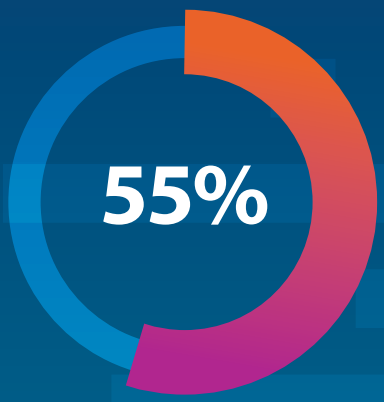
Money laundering, facilitated by individuals known as money mules, involves the illegal movement of funds obtained through criminal activities. While those in banking and finance are well-versed in Anti-Money Laundering (AML) laws, many others remain unaware of the penalties associated with aiding criminals in moving money.

Money mules, whether knowingly or unknowingly, assist in obscuring the source of illicit funds by transferring them digitally, in person, or through mail/courier services. The process typically involves the criminal transferring funds to the money mule, who then integrates them into the financial system through a series of transactions before returning the layered funds to the criminal, highlighting the ongoing challenge of combating financial crime.

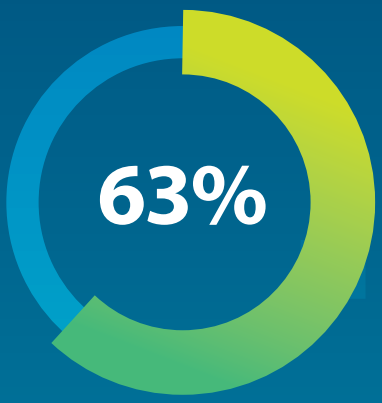
Recent data sourced from several global banks reveals consistent trends regarding money mule activities.



Surge in student involvement in money mule activities



Of money mule accounts are held by people under 30



Of people are unaware of consequences

Student Money Mules

A recent report[16] highlighted a 23% surge in student involvement in money mule activities, particularly notable at the onset of the academic year. Almost two-thirds (63%) of the young individuals were unaware of the potential consequences, including the risk of acquiring a criminal record, associated with participating in such illicit activities.

Money Mule Accounts Demographics

An examination of money mule accounts[17] shows that over half (55%) of these accounts are held by individuals aged 30 and below, with two in five (40%) under the age of 25, and one in five (20%) falling below the age of 21. Conversely, individuals aged 70 and above represent less than 1% of money mule accounts, and those between 60 to 70 years old comprise just 2%.

Reactive Global Efforts to Combat Money Mule Networks

Highlighting a collaborative global effort to combat money laundering, law enforcement agencies from multiple countries—bolstered by organizations such as Europol, Eurojust, INTERPOL, and the European Banking Federation (EBF)—have intensified their crackdown on money mules and their recruiters. The concerted efforts in 2022 led to the apprehension of 2,469 money mules in a widespread crackdown against money laundering.[18] In a subsequent push in 2023, 2,822 banks and financial institutions,[19] alongside law enforcement agencies from 26 countries, collaborated to tackle this persistent threat.

The crackdowns conducted in June, October, and November 2023 yielded significant results, identifying 10,759 money mules and 474 recruiters, culminating in the arrest of 1,013 individuals worldwide. These insights underscore the critical importance of continued vigilance and collaborative action to combat the scourge of money muling, safeguarding financial systems and communities worldwide.

Proactive Money Mule Detection

While just in the beginning stages of defining proactive money mule detection strategies, one of the ways different countries are addressing money mules is through legislation, where a portion of the reimbursement burden is placed on receiving banks to avoid potentially significant increases in losses resulting from inbound payments from scams at other financial institutions to money mules within their portfolios.[20]

Identifying Mule Accounts Is a Key Step in Stopping Fraudsters

- **Leverage a risk-based approach** and take advantage of machine learning that profiles the sender and recipient to more accurately detect mule activities
- **Update policies** to track beneficiary transaction velocity and unusual amounts
- **Utilize a data network** such as the Outseer Global Data Network to help share mule accounts intelligence with other organizations
- **Tap into the timely insights of web intelligence services** such as Outseer Fraud Action Services to identify confirmed mule accounts in addition to compromised email addresses that can be tied to accounts

Rising Liability Shifts

With the rapid increase in faster payment fraud, some governments are enacting or are considering legislation to ensure more support for victims, with the discussion centering around liability shift.

The UK & EU Are on the Forefront of Regulation

The UK and EU have been at the forefront of change with the introduction of the Payment Systems Regulator (PSR) and the upcoming Payment Services Directive 3 (PSD3). In late 2024, the specifics of PSD3 and the implementation of the PSR liability shift will be revealed. As these regulatory changes unfold, financial institutions should stay informed and prepare for potential adjustments in compliance requirements based on the finalized PSD3 framework.

The most important part of the liability changes is that financial institutions and payment service providers must reimburse all in-scope customers that are victims of APP scams, within certain limits. The sending and receiving financial institutions and payment service providers will share the cost of reimbursements to victims 50-50.

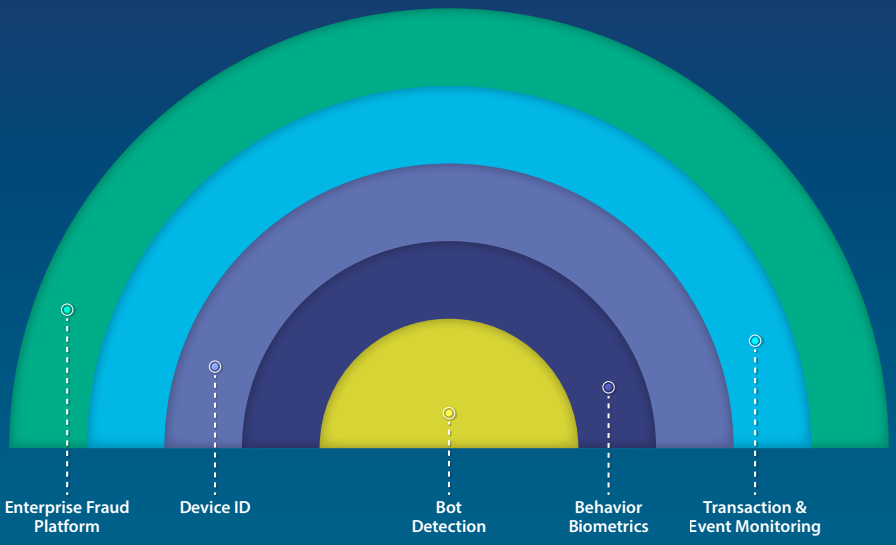
Strategic objectives of the PSR reimbursement:

1. Decrease the instances of APP fraud
2. Improve protection of payment system users
3. Incentivize payment service providers to focus on resources to prevent scams
4. Increase confidence in the Faster Payment Scheme (FPS)
5. Create agile rules to enable the operator to manage evolving fraud threats

While not mandated to adopt any regulation, those outside of the UK and EU could benefit from the learnings.

How Outseer Is Fighting Fraud

Outseer fights fraud with a comprehensive, layered approach that addresses the dynamic landscape of cyber threats. Our strategy embraces the diverse range of signals crucial for effective fraud prevention. Our solutions offer flexibility and agility, enabling swift policy adjustments without the need for extensive professional services.



Additionally, our team of Outseer Fraud Advisors ensures that your fraud prevention solutions remain fine-tuned to evolving threats, providing continuous optimization and expert guidance.

Outseer stands as your trusted partner, delivering unrivaled results through a blend of proven data science and risk engine, extensive data consortium, and adaptive resilience.

How Can Financial Institutions & Payment Service Providers Mitigate APP Fraud?

Financial institutions and payment service providers that enhance internal controls can shield themselves from liability-shift losses. Implementing controls can mitigate risk while protecting customers from fraudsters who seek to circumvent an FI's internal controls by using money mules and executing APP frauds.

In implementing a robust defense against scams, a multi-layered approach is essential. First, limiting fraudsters' access to customer credentials and Personally Identifiable Information (PII) is paramount.

And while many organizations may overlook actively tracking scams, it's crucial to track and tag scam attacks for analysis. By tracking scams, businesses can analyze data and refine their mitigation strategies accordingly. This enables a more proactive stance in identifying and countering fraudulent activities effectively.

Additionally, fostering collaboration and sharing fraud data among organizations is pivotal. Through data-sharing initiatives or fraud data consortiums, financial institutions can collectively combat fraud by leveraging shared insights. This adaptive approach ensures agility as the adoption and usage of real-time payment systems continue to grow.

Update Fraud Defenses

Tap into a data network/consortium for detection control.

Collecting more and better payment data and using that data in the context of a data network such as the Outseer Global Data Network to track crucial global data will help you better identify risk signals. Says Datos Insights, "These controls are exceptionally well positioned to be among the most effective scam detection solutions."[21]

Implement better fraud detection and prevention solutions for receive-side detection control.

Use AI and predictive analytics to facilitate fraud detection and prevention. In doing so, you can take advantage of orchestrated, risk-based smart friction to slow down risky real-time payments. These are transaction monitoring controls that are configured to predict the outcome of inbound payments.

Update your policy management.

Update policies to track transaction velocity and unusual payment amounts. Fraud detection solutions must also operate in alignment with clearly defined policies for how to manage suspect money mules and high-risk inbound payments within the constraints of regulatory restrictions and network operating rules.[22]

Update Internal Processes

What else can you do to strengthen and optimize processes and technologies to fight against APP scams?

Implement proactive prevention controls.

From customer education to internal "break the spell" teams having conversations with customers during the APP scams, there are some measures you can take proactively.

Send-side detection controls to disrupt mule account networks.

Better monitoring of money coming into as well as out of customers' accounts and analyzing the behavior of those accounts could catch fraudsters in the act.

Outseer Products

Outseer Fraud Manager

Outseer Fraud Manager is a transactional risk management platform that utilizes machine learning and a powerful policy engine to accurately assess and mitigate risk associated with each step of the digital journey.

Outseer 3-D Secure

Outseer 3-D Secure is an EMV® 3-D Secure Access Control Server (ACS) that delivers secure, frictionless digital shopping experiences your cardholders expect. 3-D Secure ensures a secure, seamless shopping experience, boosting transaction approvals, reducing fraud, and minimizing operational costs.

Outseer FraudAction

Outseer FraudAction proactively disrupt fraudulent activities, preempting harm to financial institutions, brands, and customers. Through continuous monitoring, we swiftly identify and dismantle phishing sites, malware, and social media brand abuse, while also fortifying defenses against business email compromise. Our cyber-intelligence service scours the dark web, equipping financial institutions with actionable threat intelligence reports and data feeds such as compromised credit cards and mule accounts for effective risk mitigation.

Outseer Technology

Global Data Network

Outseer's solutions harness proven data science technology and risk engine that draws insights from the Global Data Network's vast repository of billions of transactions and confirmed fraud data.

With Fraud Manager, financial institutions can streamline fraud management across the customer digital journey, optimizing risk scoring and swiftly adapting to emerging threats.

3-D Secure empowers institutions to detect more Card-Not-Present fraud with fewer interventions, thanks to predictive risk scoring and customizable challenge flows.

Sources

1 "Brand Abuse." Outseer, 2023.

2 Van Deloo, Lori. "Mobile Phishing." Outseer, 24 June 2022.

3 Moatty, Nir. "Rogue Apps: What They Are & Top Techniques to Prevent Them." Outseer, 2022.

4 GeeksforGeeks. "Generative Adversarial Network (GAN)." GeeksforGeeks, March 11, 2024.

5 "HK$200 Million Lost in Deepfake Conference Call Scam in Hong Kong First." South China Morning Post, February 4, 2024.

6 "Deepfake Scams Have Arrived: Fake Videos Spread on Facebook, Tiktok and YouTube." NBCNews.com, August 29, 2023.

7 Puig, Alvaro. "Scammers Use AI to Enhance Their Family Emergency Schemes." Consumer Advice, May 31, 2023.

8 Garner, Bethany. "What Is App (Authorised Push Payment) Fraud?" Forbes, April 9, 2024.

9 Maor, Daniel. "Hunting the Command & Control Servers." Outseer, July 28, 2023.

10 "Prime Time for Real-Time Global Payments Report." ACI Worldwide, April 16, 2024.

11 BIS Quarterly Review, March 2024. Accessed March 2024.

12 Conroy, Julie, Trace Fooshée, and David Mattei. "Faster Payments, Faster Fraud." Aite-Novarica, May 2023.

13 "Annual Fraud Report 2023." UK Finance.

14 "Growth in APP SCAMS Expected to Double by 2026 – Report by ACI Worldwide and GlobalData." Business Wire, November 15, 2022.

15 "New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022." Federal Trade Commission, February 23, 2023.

16 "Barclays Warns of 23 per Cent Surge in Student Money Mules." Barclays.

17 "About Santander UK." Santander UK, October 26, 2023.

18 "2,469 Money Mules Arrested in Worldwide Crackdown against Money Laundering." Europol.

19 Barbieri, Vittoria. "Paper Trail Ends in Jail Time for 1013 Money Mules: 2822 Banks and Financial Institutions Join Forces with Law Enforcement Agencies in Global Effort against Money Laundering." EBF, December 4, 2023.

20 "Marketplace Trends in Authorized Payment Fraud Controls." Datos Insights, March 2024.

21 Ibid.

22 Ibid.

OUTSEER

At Outseer, we are empowering our customers to liberate the world from digital fraud by providing solutions that stop fraud, not customers. Our market-leading fraud and authentication platform is used by thousands of financial institutions around the world to protect millions of customer accounts and billions of transactions annually. Leveraging proven data science, including our proprietary consortium data, our customers use our risk-based, machine learning platform to deliver the highest fraud detection rates, lowest false positive rates, and lowest customer intervention in the industry. See what others can't at outseer.com.

Serve over **400 customers** across **~50 countries**

More than 20 years of incumbency protecting **trillions of global transactions**

Serve **24 of the top 50** global financial institutions

~400 employees with concentrations in India, Israel, US, and UK

$5T+
annual protected payments

100B+
transactions and digital interactions protected annually

$450M+
cards and bank accounts protected

rev. 04-30-24