FIRST HALF OF 2022 (1H 2022)

Outseer™ Fraud & Payments Report

Digital transaction insights from the Outseer Global Data Network™

OUTSEER

Research Note

The Outseer™ Fraud & Payments Report presents an analysis of fraud attack and consumer fraud data collected by the Outseer team while identifying threats for Outseer customers globally. As such, it provides a glimpse into the cyber fraud landscape for consumer-facing organizations of all sizes and types. Outseer solutions have protected thousands of organizations and billions of consumers globally for over twenty years. Outseer's precision detection allows the largest financial institutions globally to maximize revenues by reducing fraud losses and increasing transaction approval rates.

Table of Contents

Outseer observed several global fraud trends across attack vectors and digital channels in the first half of 2022

The highlights include:

As Card Not Present (CNP) volume continues to grow so does the usage of EMV® 3-D Secure (3DS). 3DS is an effective tool to mitigate CNP Fraud while increasing authorization rates and cardholder satisfaction:

- During the six months ending June 2022, **Outseer 3-D Secure™ protected over $110 Billion in 3DS payments volume.** In the same period, Outseer 3-D Secure saw 34% growth in protected transactions compared to the same period in 2021.
- **Merchants' adoption of the EMV® 3DS globally grew 137%** from January 2022 to June 2022.
- **In the UK, a 62% spike in the number of merchants sending transactions** through the EMV 3DS rails between February 2022 and March 2022 when PSD2 SCA for eCommerce transactions enforcement date came into effect.
- **Scams resulting in Authorized push payments (APP) fraud are on the rise**. 75% of fraud value in online banking payments came from a trusted account and trusted device during Q2 2022.
- **~87,000 attacks were detected by Outseer FraudAction™**. This is equivalent to an average of almost 20 attacks detected every hour!
- **Over 2.7 Million compromised cards were detected** by the Outseer FraudAction team during the first half of 2022.
- **Brand Abuse attacks are still the most observed attack**, representing 65% of all attacks in the first half of 2022. Other attacks included: Phishing (18%), Rogue mobile apps (14%) and Trojans (3%).

1H 2022 Key Trends

EMV® 3DS Usage Continues to Scale

34%
increase in protected 3DS transactions in 1H 2022

$110B
3DS Payments Volume protected in 1H 2022

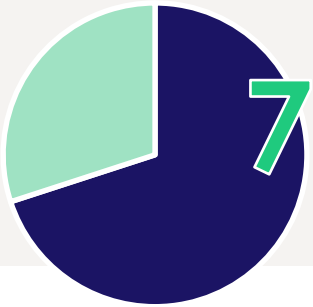
277%
growth in number of Merchants using EMV® 3DS globally *(June 2021 vs June 2022)*

Scams and Social Engineering Fraud Are on the Rise

75% of online banking payments fraud ($) occurred on a trusted account and trusted device – indicative of APP Fraud

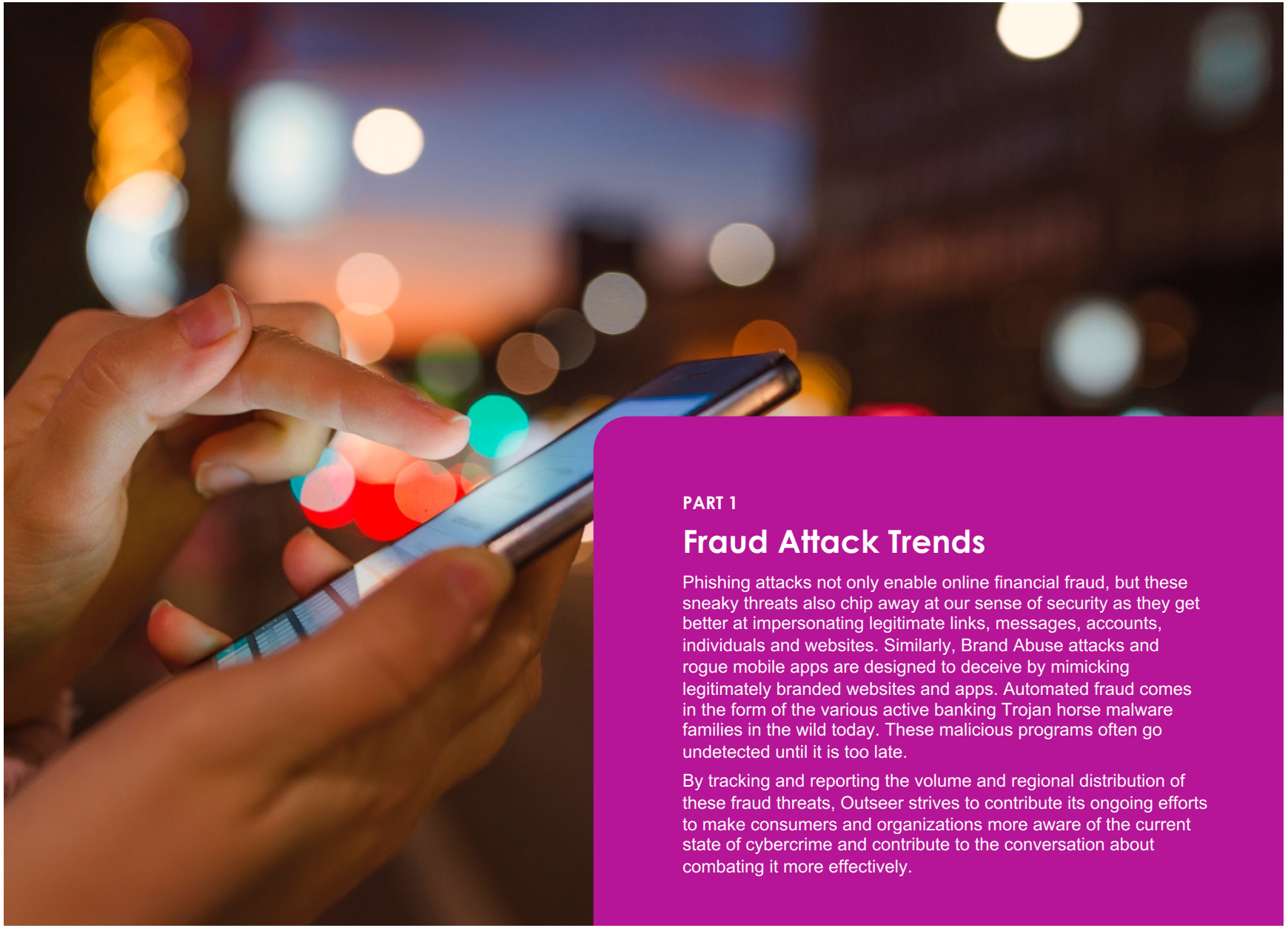
87,000
Attacks detected by Outseer FraudAction™, 65% of these attacks are attributed to Brand Abuse

Most digital banking fraud originated in the mobile channel



70% of fraudulent transactions in online banking originated from the mobile channel

Source: Outseer Research 2022



PART 1

Fraud Attack Trends

Phishing attacks not only enable online financial fraud, but these sneaky threats also chip away at our sense of security as they get better at impersonating legitimate links, messages, accounts, individuals and websites. Similarly, Brand Abuse attacks and rogue mobile apps are designed to deceive by mimicking legitimately branded websites and apps. Automated fraud comes in the form of the various active banking Trojan horse malware families in the wild today. These malicious programs often go undetected until it is too late.

By tracking and reporting the volume and regional distribution of these fraud threats, Outseer strives to contribute its ongoing efforts to make consumers and organizations more aware of the current state of cybercrime and contribute to the conversation about combating it more effectively.

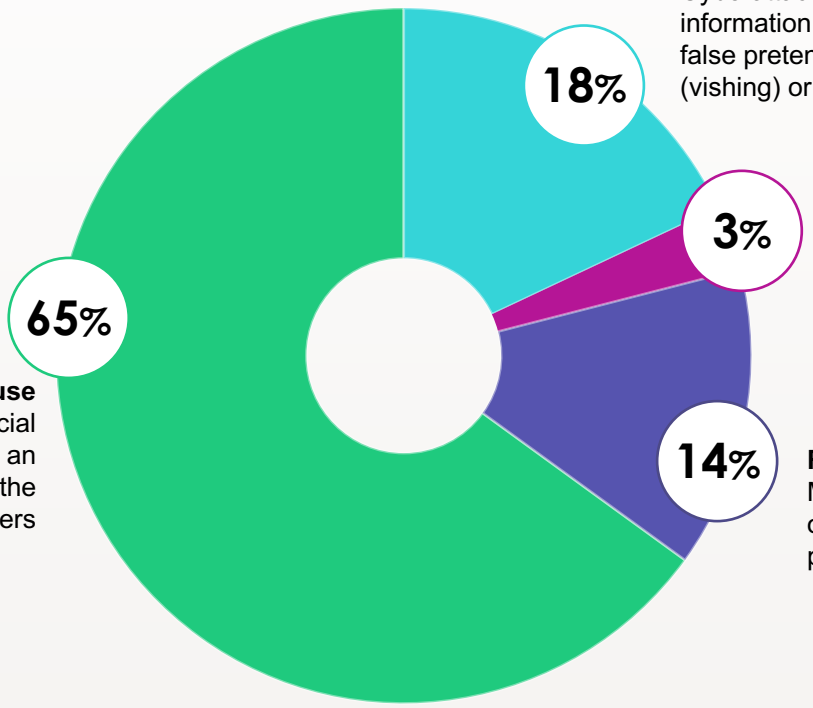
1H 2022 Fraud Attacks Distribution

Outseer identified almost 87,000 attacks worldwide in the first half of 2022.

Brand Abuse attacks continue to be the most-dominant attack with 65% of all attacks detected in the first half of 2022 belonging to this category.

87,000

Attacks detected during the first half of 2022



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

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

Rogue Mobile Apps
Mobile applications using an organization's brand without permission

Brand Abuse
Online content, such as social media, that misuses an organization's brand with the purpose of misleading users

Source: Outseer FraudAction Research

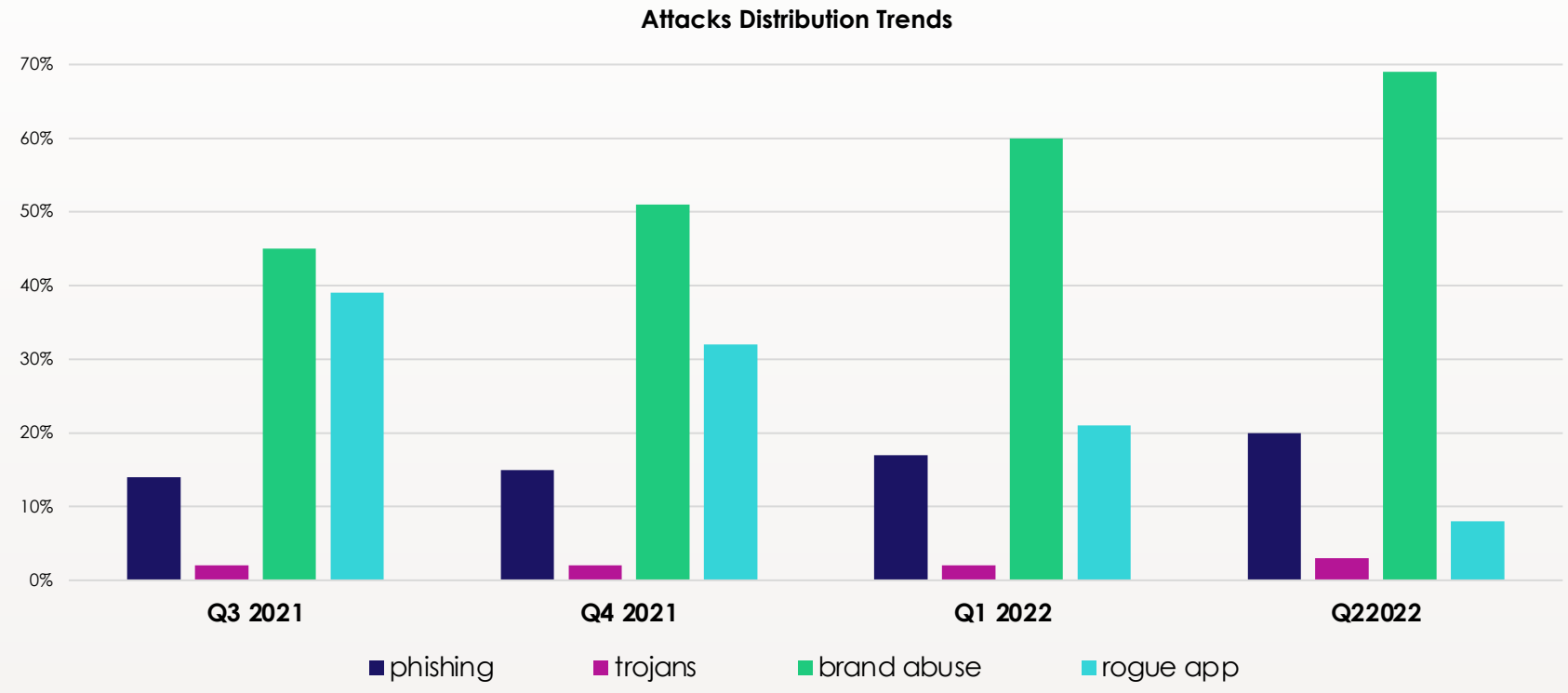
Attacks Distribution Trends

Over the last four quarters, we've observed an increasing trend in Brand Abuse attacks, decreases in Trojan attacks, and relatively flat Phishing activity.

Fraudsters are impersonating organizations to mislead consumers, which not only harms the organization's brand but also compromises consumer data which can be used in account takeover attacks.

The rise in Brand Abuse attacks could be due to their simplicity, as they are relatively easy to execute; all fraudsters need is a convincing web page, compared to rogue mobile apps which require an entire app to be developed.

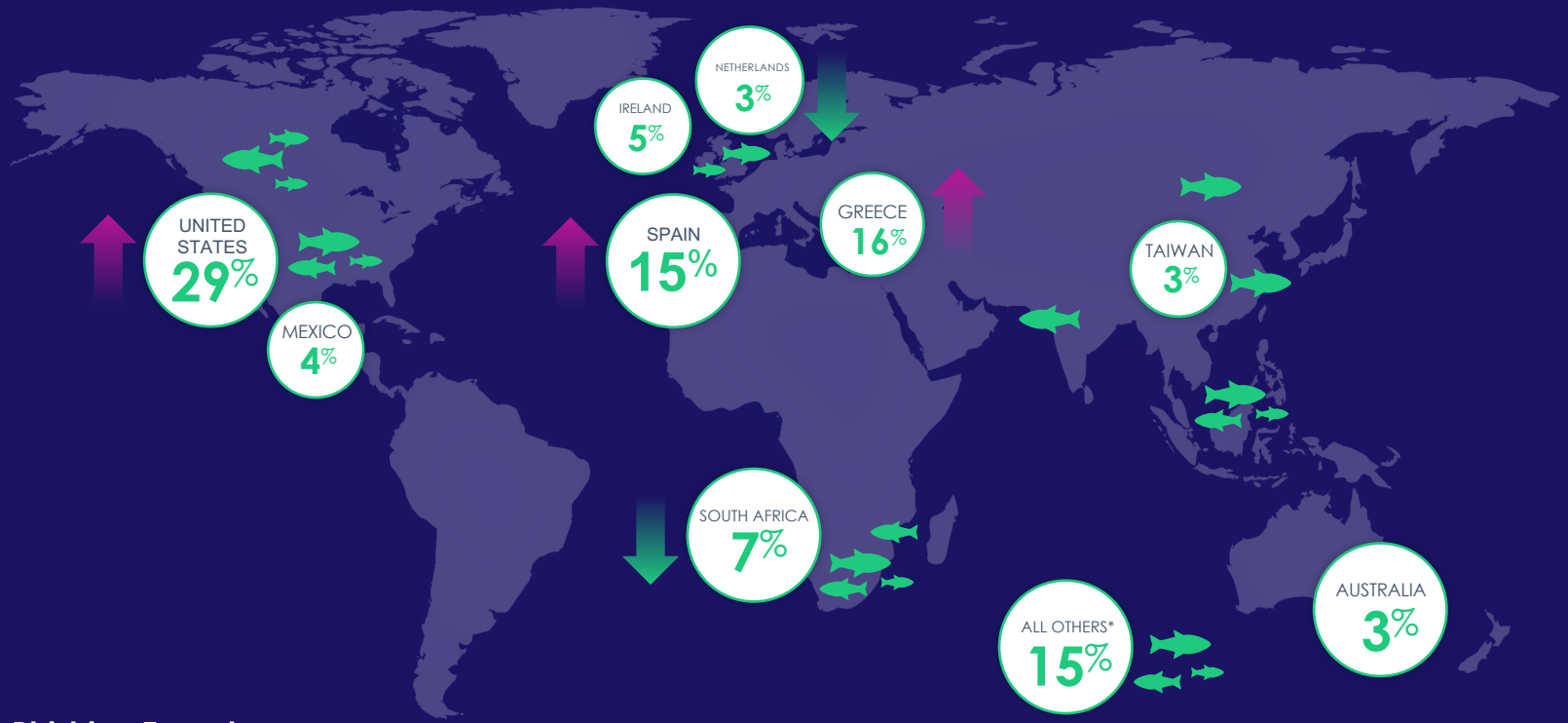
Organizations of all sizes are heavily advised to monitor their brand and their executives, either by themselves or by leveraging a brand abuse protection service that can rapidly detect and shut down such attacks. The faster an attack is detected and taken down, the less impact it has on the organizations' brand and customers.



Source: Outseer FraudAction Research 2021-2022

FRAUD ATTACK TRENDS

Top Phishing Target Countries



Phishing Targets

In Q2 2022, the Outseer FraudAction team identified the United States as the most targeted country for phishing attacks. The number of phishing attacks targeting the US grew 42% in the first half of 2022 when compared to the same period in 2021.

Source: Outseer FraudAction Research Q2 2022

FRAUD ATTACK TRENDS

Top Phishing Hosting Countries

1 United States

2 Russia

3 Germany

4 France

5 India

6 United Kingdom

7 Malaysia

8 Brazil

9 Hong Kong

10 Canada

Phishing Hosts

The United States remains the top hosting country for phishing attacks accounting for 79% of Internet Service Providers (ISPs) hosting these types of attacks in Q2 2022.

Phishing attacks originating in Russia grew 25% in the first half of 2022 when comparing to the same period in 2021; this might be a result of the cyberwar that we witness alongside the ground war with Ukraine.

Source: Outseer FraudAction Research Q2 2022

Compromised Cards Discovered/Recovered by Outseer

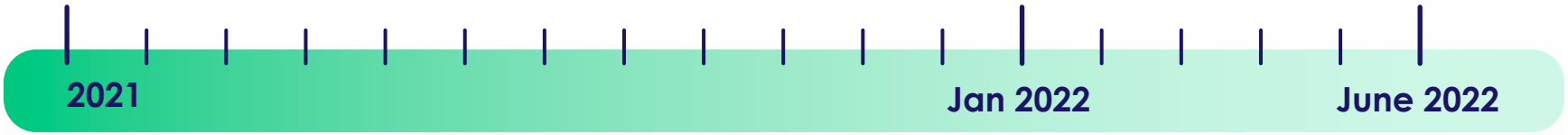
Outseer's FraudAction™ service discovers CVV2-related data, which is card data compromised through cyberattacks targeting online transactions or e-commerce. This type of data can be exploited for use in a variety of fraudulent activities, including "carding," which refers to using compromised cards to buy goods both in physical stores and on e-commerce websites.

During the first half of 2022, Outseer recovered over 2.7 million unique compromised cards and card previews from online card stores and fraud communication channels.

During the 18-month period ending June 2022, Outseer recovered over 16.5 Million cards

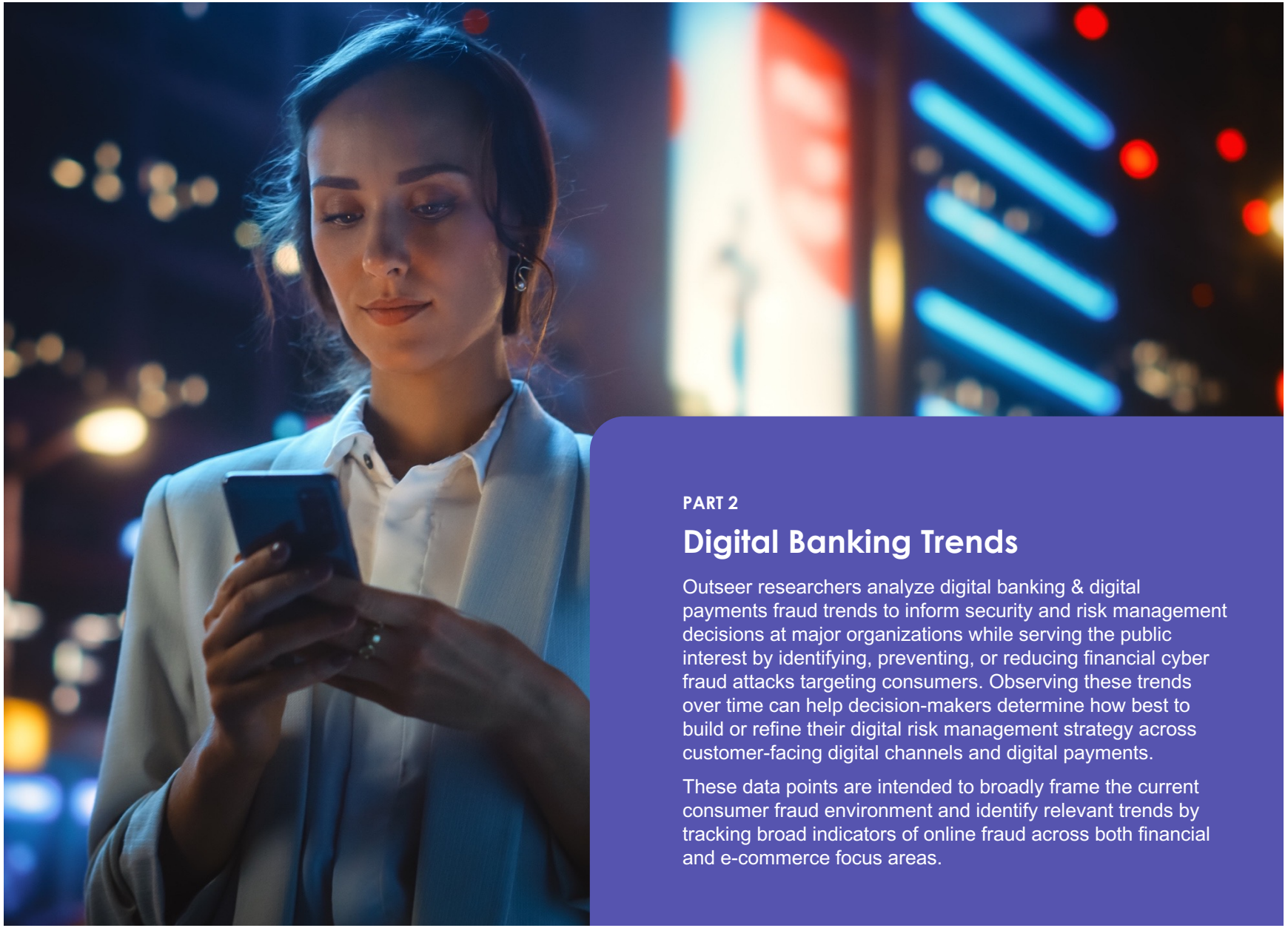
2.7M

Unique compromised cards & card previews recovered during the first half of 2022



16.5M

Cards recovered during an 18-month period



PART 2

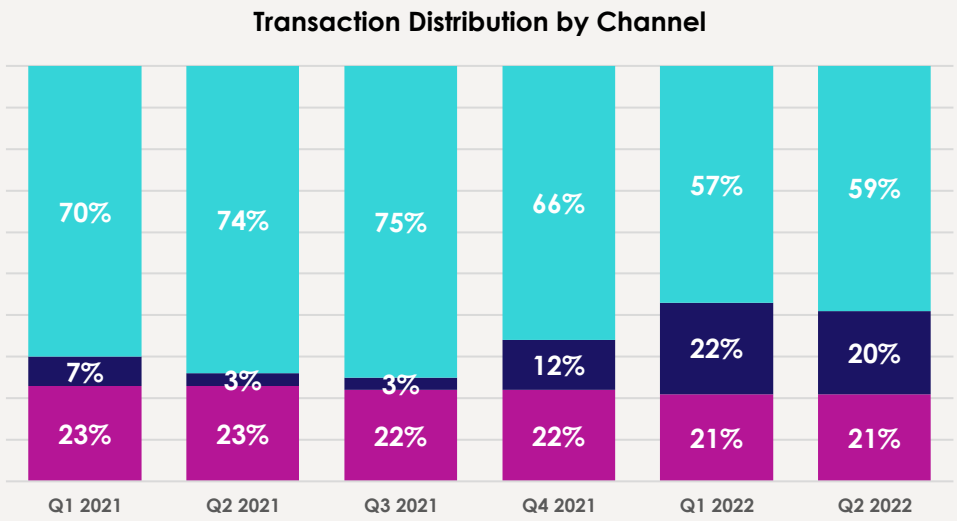
Digital Banking Trends

Outseer researchers analyze digital banking & digital payments fraud trends to inform security and risk management decisions at major organizations while serving the public interest by identifying, preventing, or reducing financial cyber fraud attacks targeting consumers. Observing these trends over time can help decision-makers determine how best to build or refine their digital risk management strategy across customer-facing digital channels and digital payments.

These data points are intended to broadly frame the current consumer fraud environment and identify relevant trends by tracking broad indicators of online fraud across both financial and e-commerce focus areas.

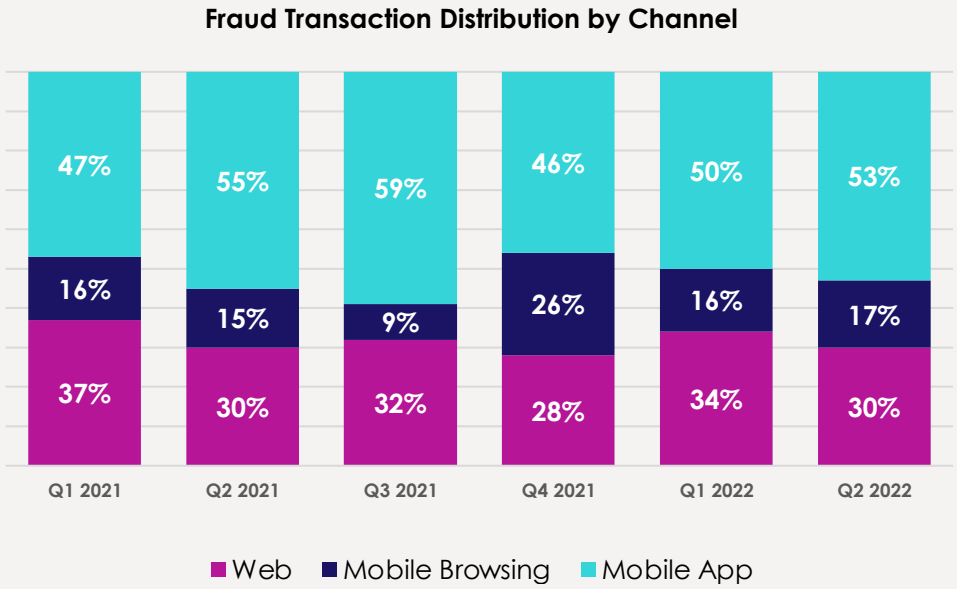
Digital Banking Transactions Distribution by Channel

Mobile banking (mobile browsers or mobile apps) continues to be the dominant channel for digital banking with **79% of digital transactions in the first half of 2022** originating in the mobile channel. Most of the mobile banking transactions originated from a mobile application.



Digital Banking Fraudulent Transaction Distribution by Channel

While 79% of digital banking transactions originated from the mobile channel in Q2 2022, the mobile channel is accountable for **70% of fraudulent online banking activities**, a slight increase from 66% in Q1 2022.



Source: Outseer Research 2021-2022

Credit Cards & Digital Payments: Average Transaction and Fraud Transaction Values

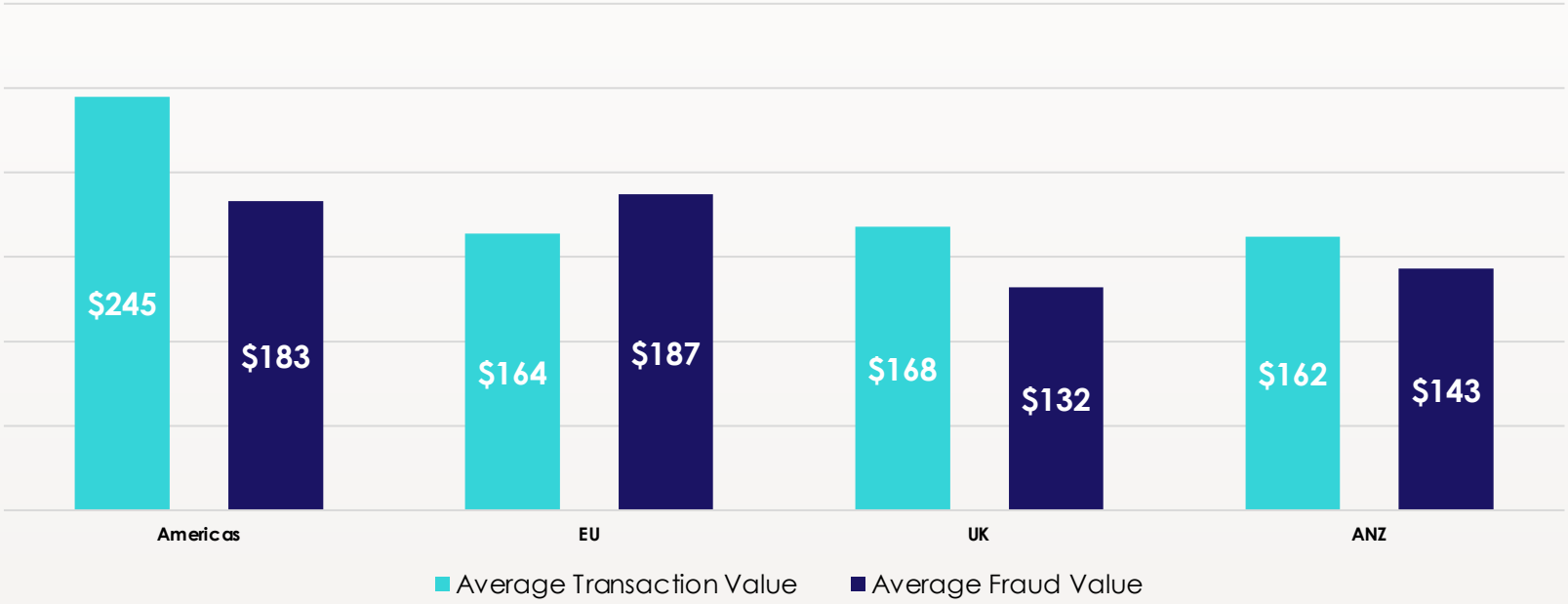
Outseer observed the highest average transaction value in the Americas. In fact, the average e-commerce transaction value in the Americas is 150% higher than the average e-commerce transaction value in the EU. However, the Average Fraud Value observed was similar between the Americas and the EU.

In addition, in the Americas the average value of fraudulent e-commerce transaction is over 2.5 times higher for Debit cards ($467) than it is for Credit card ($183).

Average fraudulent transaction size is decreasing in the UK quarter after quarter, which may be the result of PSD2 regulation. Just like the shift in fraud that was observed when Chip & Pin was rolled out in the UK and fraud shifted to the US, we expect similar trend with CNP fraud where the high adoption of EMV® 3DS in the UK & EU makes fraudsters shift to the US. In fact, an Aite-Novarica Group research estimates that CNP Fraud losses will decrease 35% in the EU in 2023 compared to 2020 while in the US CNP fraud is expected to increase 28% in the same period.[1]

1 Aite-Novarica Group, Maximizing the potential of CNP. October 2021

Average Credit Card Transaction Values



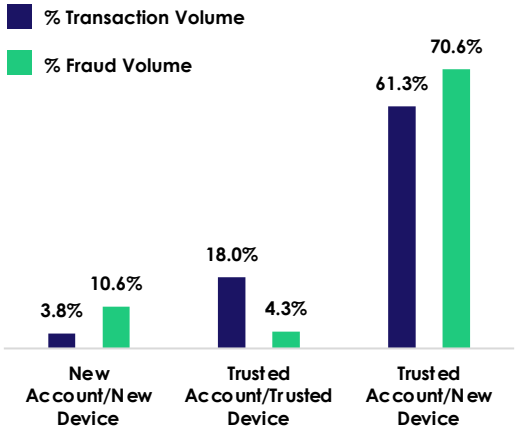
Source: Outseer Research Q2 2022

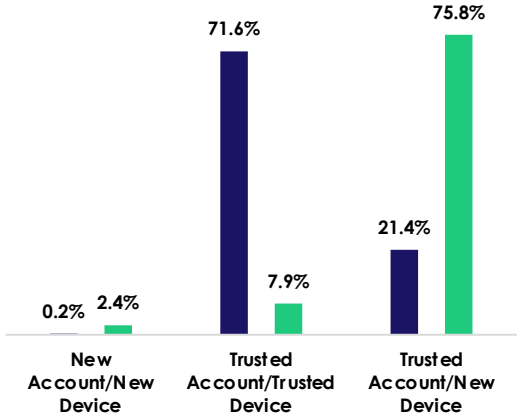
Device Age vs. Account Age

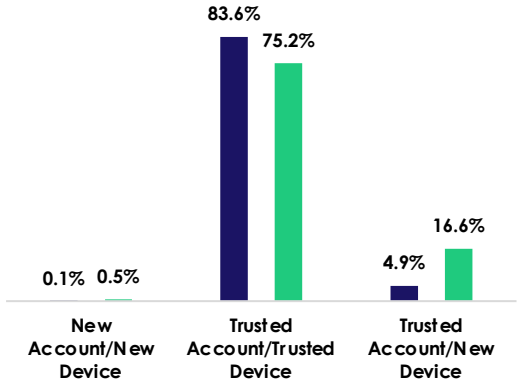
Device Age refers to how long the Outseer Platform has “known” or “trusted” a given device (laptop, smartphone, etc.).

Account Age refers to how long the Outseer platform has “known” or “trusted” a given account (login, etc.).This data demonstrates the importance of accurate device identification to minimize false positives and customer friction during a login or transaction event.

Analysis: In many cases, fraud originated from a trusted account and a new device is indicative of Account Takeover attacks while fraud originated from a trusted account and trusted device is indicative of scams and authorized payments (APP) fraud.







E-Commerce

Fraudulent transaction value originating from a trusted account and trusted device grew from an average of 2% in the first half of 2021 to over 4% in the first half of this year (2022), however the majority of CNP fraud (over 70% of fraud value) that was observed in the first half of this year came from a trusted account and new device which is indicative of account takeover.

Login

Logins from a new device and trusted account were accountable for over 75% of fraud value for online banking logins at Q2 2022 which indicates that account takeover is still the most common fraud attack at login.

Payment

The highest percentage of fraudulent online payment value was observed from a trusted account and trusted device, in Q2 2022 over 75% of online banking payments fraud originated from this category. This is indicative of an increase in scams resulting in authorized payments fraud (APP) as the fraudsters apply social engineering to manipulate the genuine user to pay from his/her account; the payment is completed from the genuine user’s device by the genuine user who was misled by fraudsters.

Source: Outseer Research Q2 2022

PART 3

CNP & Digital Payments Trends

The acceleration of digital transformation is driving the introduction and/or scaling of new digital commerce models across the spectrum of pay before (e.g., buy on mobile pick up in store) pay now (e.g., pay @ the table) and pay later (e.g., Buy now, pay later options. As new models scale, card issuers and payments processors must be prepared for the increased payment risks and challenges that come with them. At the same time, increasing transaction approval rates is key for business growth. This section includes trends in 3DS Card Not Present (CNP) transactions as observed by the Outseer team.

Merchant Adoption of EMV® 3DS is on the Rise Globally

Adoption of EMV® 3DS by merchants and card issuers can help increase transaction approval rates while keeping fraud loss and chargebacks low. Higher approval rates translates into higher interchange revenues.

Outseer observed a dramatic increase in the number of merchants using EMV® 3DS by tracking unique merchant IDs that are initiating 3-D Secure transactions protected by Outseer 3-D Secure. The Outseer team observed a 137% increase in the number of unique merchants (Globally) using EMV® 3DS between January and June 2022.

Specifically in the US, a 146% increase in the number of US merchants sending EMV® 3DS transactions was observed by Outseer when comparing January 2022 to June 2022.

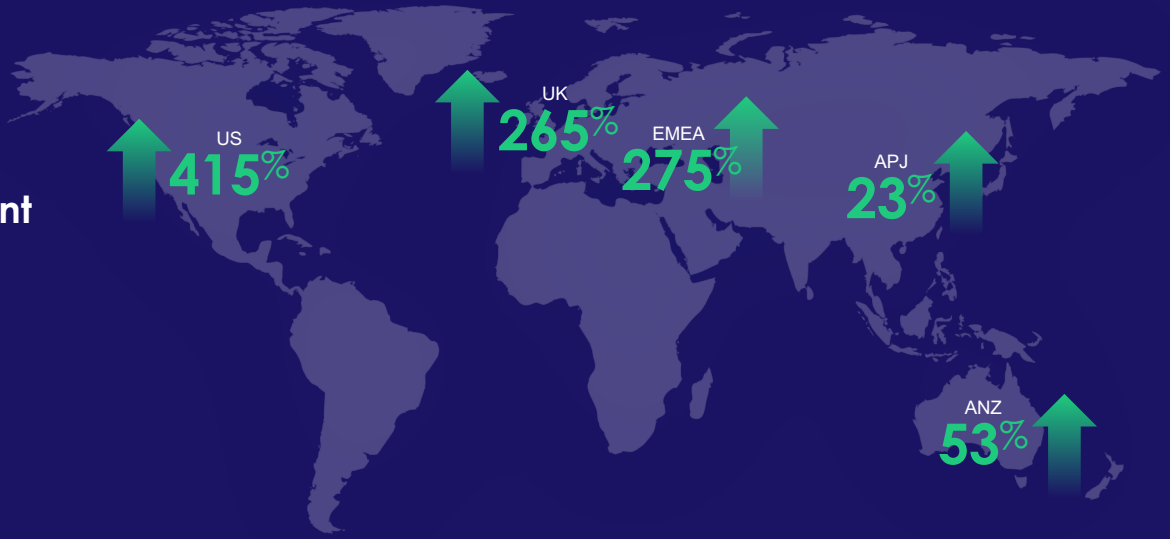
There was an 62% Increase in the number of UK Merchants sending EMV® 3DS transactions from February to March 2022. This is likely the result of the PSD2 Strong Customer Authentication (SCA) enforcement date coming into effect in the UK in March 2022.

+277% Growth
in number of **merchants using EMV® 3DS globally** when comparing June 2021 to June 2022

+2.3 Million Merchants
are using **EMV® 3DS globally by end of June 2022**

+137%
increase in the number of unique merchants globally using EMV® 3DS between January and June 2022

Global Growth in Merchant Adoption of EMV® 3DS
(12 months ending June 2022)



Source: Outseer Research 2021-2022

Global EMV ® 3DS Transaction Growth Continues

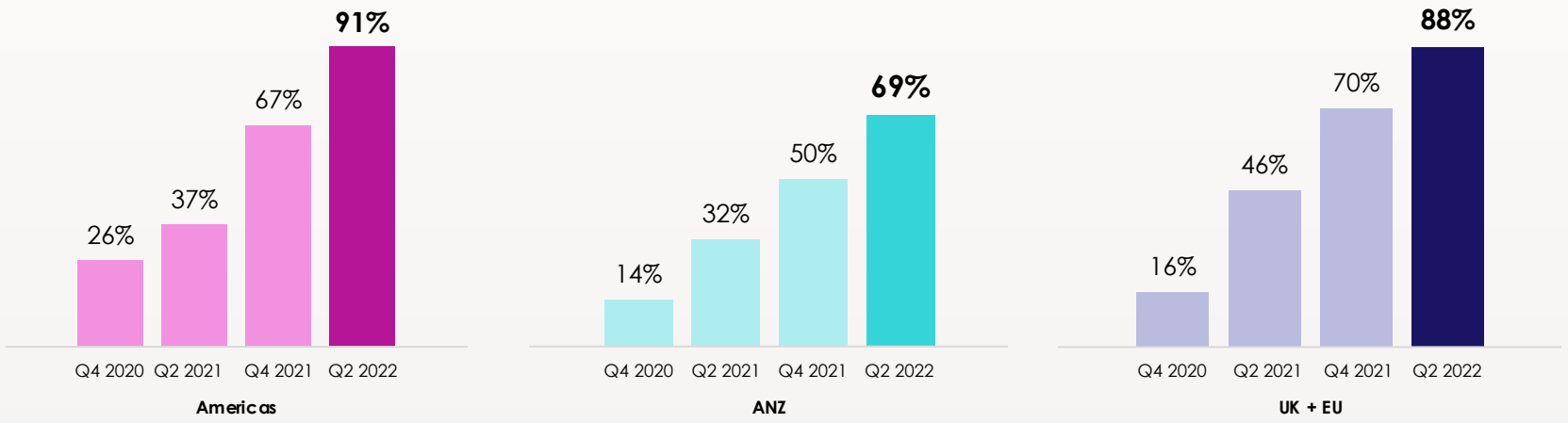
Outseer continues to observe clear, steady increases in EMV® 3DS transaction volumes across all geographies. Outseer has seen quarter on quarter increases with the Americas and United Kingdom plus Europe (UK+EU) reaching 91% and 89%, respectively by the end of 1H 2022.

Merchants in Australia and New Zealand (ANZ) have been somewhat slower to transition to EMV® 3DS. Based on results of the recent Aite study, 67% of merchants who were not yet transitioned to EMV ® 3DS globally indicated their intention to transition by the end of 2022.

REMINDER:
Sunsetting of 3DS v1.x Deadlines

- Card Networks are sunsetting support in October 2022
- The Networks are providing extensions in some countries
- **Upgrade to EMV® 3DS now**

EMV ® 3DS transactions out of all 3DS transactions



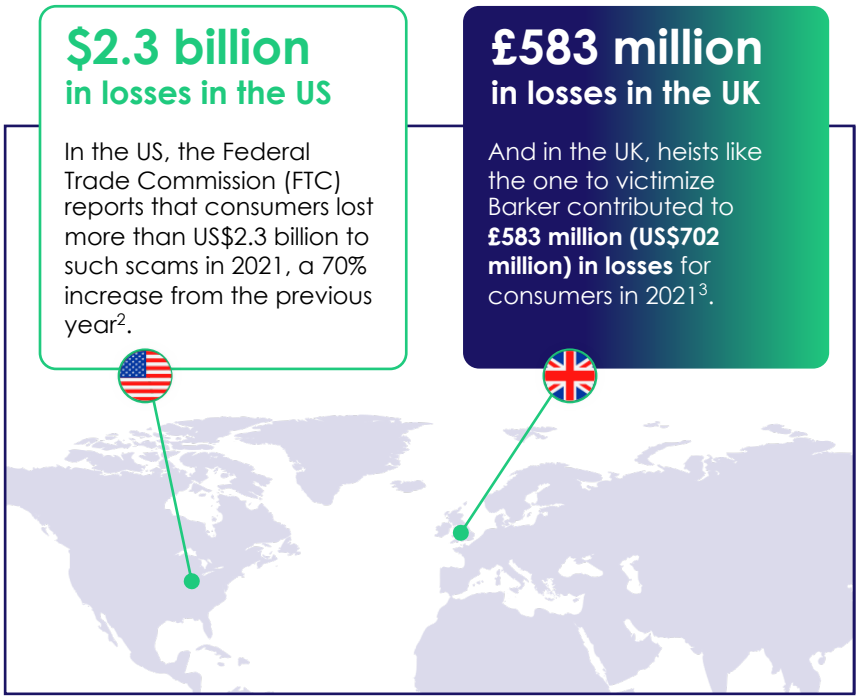
Source: Outseer Research, 2020- 2022

FEATURE ARTICLE

Fast & Furious: Hitting the Brakes on Authorized Push Payment (APP) Fraud

Mary Barker, new retiree, recently told The Guardian[1], life as she knew it ended abruptly when she was scammed into transferring £70,000 (US$84,250) to fraudsters. Barker decided to invest in a bond offering from a well-known financial firm. Much to her horror, she would later discover that cybercriminals had cloned the firm's website and paperwork and duped her into transferring half her life savings into an account under their control.

Unfortunately, she's not alone…



Indeed, APP scams are downright pernicious. Card-not-present (CNP) fraud and illicit transactions made in an account takeover (ATO) attack are forms of unauthorized payment schemes. By contrast, APP scams occur when fraudsters deceive consumers or businesses into making a payment or wire transfer to the perpetrators' accounts under false pretense.

Since these ill-advised payments are initiated by a legitimate account holder, they are, by definition, authorized. And because they originate from the account holder's own device, the duplicity behind these transactions is notoriously difficult to detect and disrupt.

Take The Money & Run

To be clear, the victims of these crimes shouldn't be dismissed as negligent or gullible. Authorized push payment scammers leverage highly-sophisticated social engineering techniques to impersonate well-known brands or individuals and exploit misplaced trust. APP fraud also takes many different forms.

Common modalities include:

- BOGUS ACCOUNT ALERTS
- P2P PLOYS
- INVOICE FRAUD
- REAL ESTATE WIRE FRAUD
- ROMANCE SCAMS
- MONEY MULE SCAM
- CRYPTO CONS

The Blame Game Has No Winners

By most accounts, victims of APP fraud aren't often pleased with banks[4] reaction to their plight.
Many transactions are instant and irrevocable. Yet while most financial institutions cover the cost of *unauthorized* payment fraud, they're reluctant to refund transactions that customers initiate themselves.
With APP fraud beginning to outpace CNP fraud and other forms of unauthorized payment fraud, it's unclear how long the cold-shoulder approach will fly.

- In the UK, proposed legislation would require banks to cover APP scam losses[5],—and publish data on their performance in reimbursing victims and shutting down accounts used to receive fraudulent funds (just 46% of losses have been reimbursed under an existing voluntary scam code[6])
- Additional legislation would also hold social media platforms and search engine companies accountable for failing to identify and remove fraudulent online advertising that often includes APP scams.
- In the US, the Consumer Financial Protection Bureau (CFPB) is moving to expand application of federal law covering reimbursement for unauthorized electronic funds transfer to include certain forms of APP fraud[7]

There's also the inevitable reality check:

Pinning the blame for APP fraud on duped customers is never going to be a winning strategy—regardless of the regulatory environment. The reputational harm from failing to act will boil into a competitive threat. To be viewed as trusted safe-keepers of their customers' money, organizations must find ways to prevent customers from falling victim to scams. Even when that means protecting customers from themselves.

Stopping Criminals, Not Customers

There is no panacea, no single, bulletproof solution that can protect against every form of APP scam. But there are meaningful steps banks, credit card companies, and other FIs can take to mitigate this growing threat.

- Protect every step of the user digital journey, from login to money transfer and any edits to the user credentials should be evaluated, this way you can gain holistic view on your customers and better protect them from their own mistakes.
- Understand and get ahead of compliance mandates and take appropriate steps to meet or exceed them.
- Educate customers about this risk—including onscreen warnings during digital transactions, “are you sure you know the person you are transferring money to?”
  if you get your customers to think for one more second before they authorize the payment, you might save them time, money and needless pain.
- Source a cyberattack detection and takedown service to stop impersonation scams before they cause harm.
- Participate in consortiums that operate across industries, geographies, governments, and law enforcement authorities to share data on fraud, transactions, and mule accounts to help detect and disrupt cybercriminals.

Providing Bigger Value

Making inroads against APP fraud can pay big dividends, instead of perpetuating the notion of an uncaring, faceless institution, you're adding value to the customer's life—by protecting them from fraudsters, and from making costly mistakes. Protecting every step of the customer journey while allowing customers to interact and transact seamlessly will sufficiently differentiate your brand and help your organization grow the bottom line.

About Outseer

Outseer empowers the digital economy to grow by authenticating billions of transactions annually. Our payment and account monitoring solutions increase revenue and reduce customer friction for card issuing banks, payment processors, fintech providers and merchants worldwide. With more than 20 billion annual transactions and 1000+ global institutions contributing to the Outseer Global Data Network, our identity-based science delivers the highest fraud detection rates and lowest customer intervention in the industry.

FEATURE ARTICLE SOURCES

1 The Guardian: Victimhood

2 Payments Dive

3 Global Banking & Finance

4 Forbes

5 Pymnts 1

6 The Guardian: V: 700000

7 Pymnts 2

8 Pymnts 3

OUTSEER