Outseer™ Fraud & Payments Report

Q3 2021

Digital Transaction Insights from the Outseer Global Data Network™

OUTSEER
An RSA Company

Table of Contents

Executive Summary

The **Outseer^{TM} Fraud & Payments Report** presents a global analysis of fraud attacks based on consumer fraud data collected by the Outseer team. It provides insight into the cyber fraud landscape for consumer-facing organizations of all sizes and categories.

Outseer-observed Fraud Attacks and Consumer Trends

Q2 2021 highlights:

- The Outseer FraudAction™ team detected more than 49,000 fraud attacks during Q2 2021
- For the third quarter in a row, brand abuse continues to be the most prevalent attack vector observed by Outseer. Fraudsters are leveraging social media to harvest users' credentials and personally identifiable information (PII)
- The number of rogue mobile apps uploaded to popular app stores spiked 66% in Q2, up 140% from the same period last year (Q2 2020). Cybercriminals create imposter banking apps to infect consumers’ devices with malware capable of harvesting user credentials for use in account takeover attacks
- Outseer recovered more than 4.5 million unique compromised cards and card previews from elicit marketplaces and communications channels in Q2 2021
- 70% of fraudulent digital banking transactions originated in the mobile channel during Q2, with mobile banking app fraud accounting for the largest increases
- In 2021, Outseer processed more than $100 billion in payment volume through its Outseer 3-D Secure^{TM} (3DS) product. Share of EMV® 3-D Secure (3DS) usage continues to show strong growth across all geographic regions

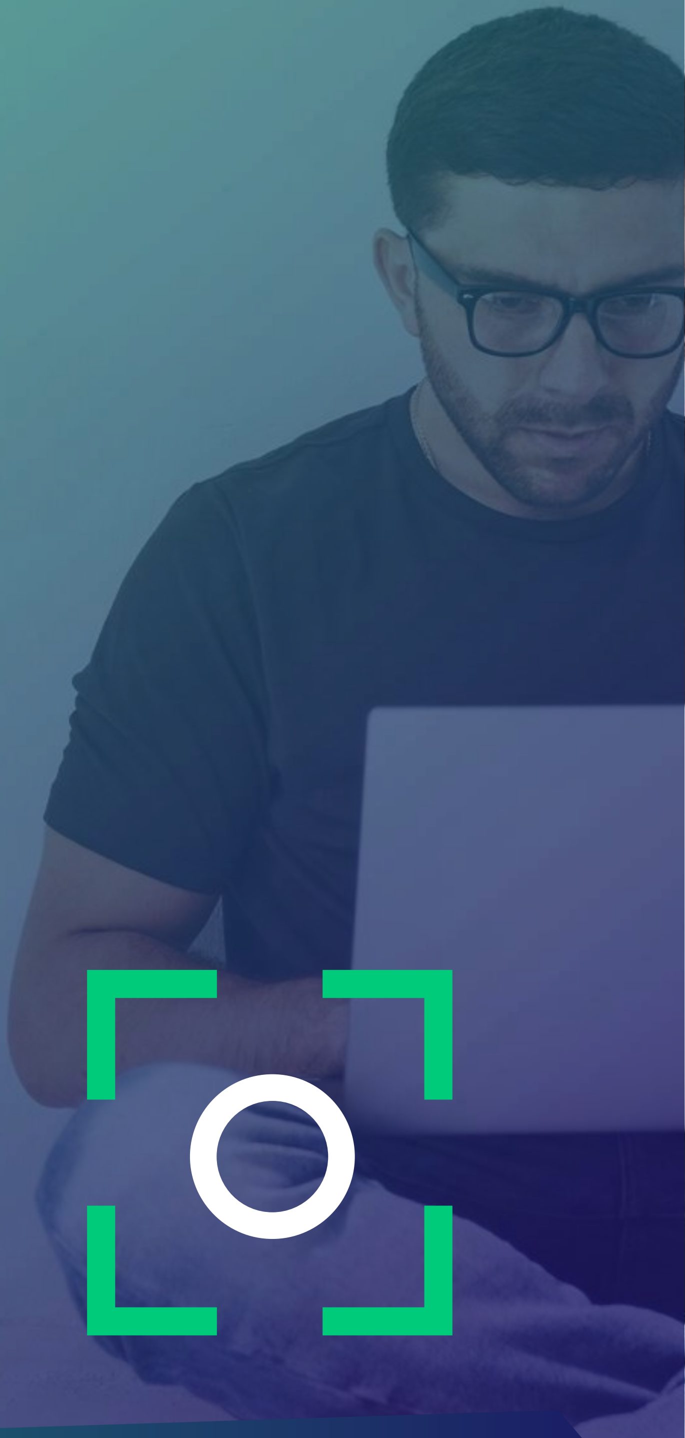
PART 1

Fraud Attack Trends

Digital transformation is reshaping nearly every facet of our lives – how we live, how we shop and who we trust. As new digital models scale, organizations must be prepared for the potential risks and challenges that may come with them.

Based on data analyzed by the Outseer Data Science and Research teams, a number of notable fraud activities have been identified across attack vectors and spanning all digital channels.

By tracking and reporting the volume and regional distribution of these fraud threats, Outseer seeks to help build awareness about the current state of cybercrime and advance the conversation about combating it more effectively.



FRAUD ATTACK TRENDS: OVERVIEW

Fraud Attack Type Distribution

Outseer identified over 49,000 attacks worldwide in Q2 2021. For the third consecutive quarter, brand abuse attacks were the most dominant attack vector observed by Outseer, representing about half of all attacks.

The growth and prevalence of brand abuse mirrors the increased use of digital platforms. Social media sites, the web, and cloud-based collaboration tools utilized by consumers and organizations are all fertile hunting ground for fraudsters. As digital transformation continues to accelerate, brand abuse is likely to proliferate and become more sophisticated.

100,000+

Attacks detected in 2021

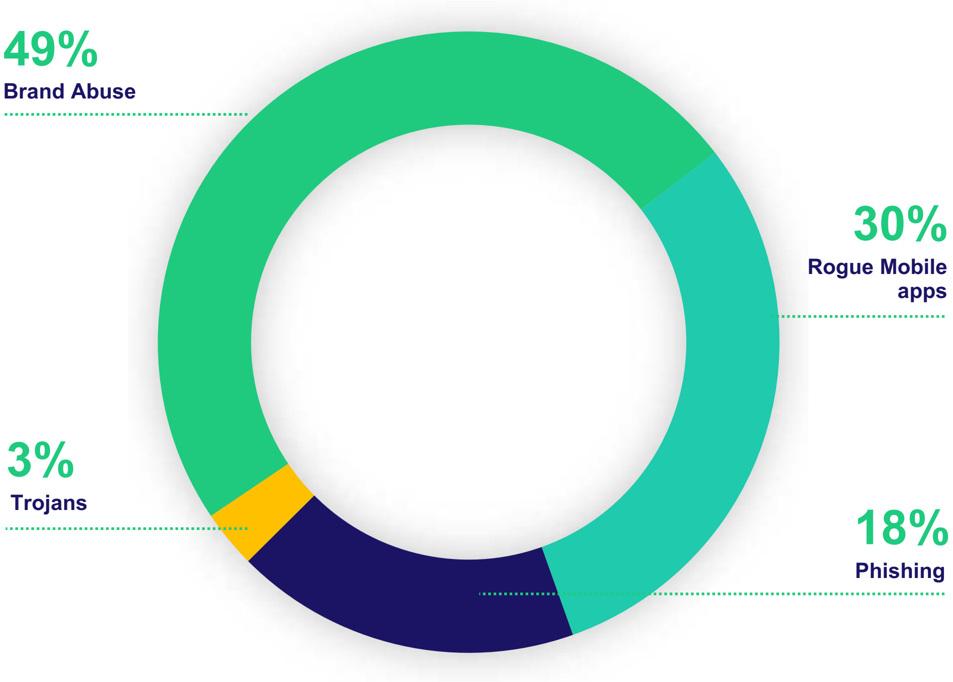
Rogue mobile apps accounted for 30% of all attacks seen by Outseer in Q2 2021 – a spike of 66% in just 90 days. That's also a 140% increase over the same quarter last year (Q2 2020). This growth may be attributable to consumers' increasing use of mobile banking apps, as fraudsters look to monetize this trend.

Fraudsters create phony banking apps and upload them to app stores to infect consumers' devices with malware capable of harvesting user credentials for use in account takeover schemes. Organizations should consider monitoring authorized and unauthorized app stores or use third-party monitoring and detection services to protect their brands and their customers.

Phishing activity remains prominent worldwide, representing 18% of all attacks. Meanwhile, Trojan attacks continue to decline, representing only 3% of the total, as criminals continue to shift attack strategies.

Source: Outseer FraudAction Research

Fraud Attacks Worldwide



Source: Outseer Research April – June 2021

Fraud Attack Glossary

Brand Abuse
Online content designed to impersonate trusted brands with the purpose of misleading users in digital channels such as social media.

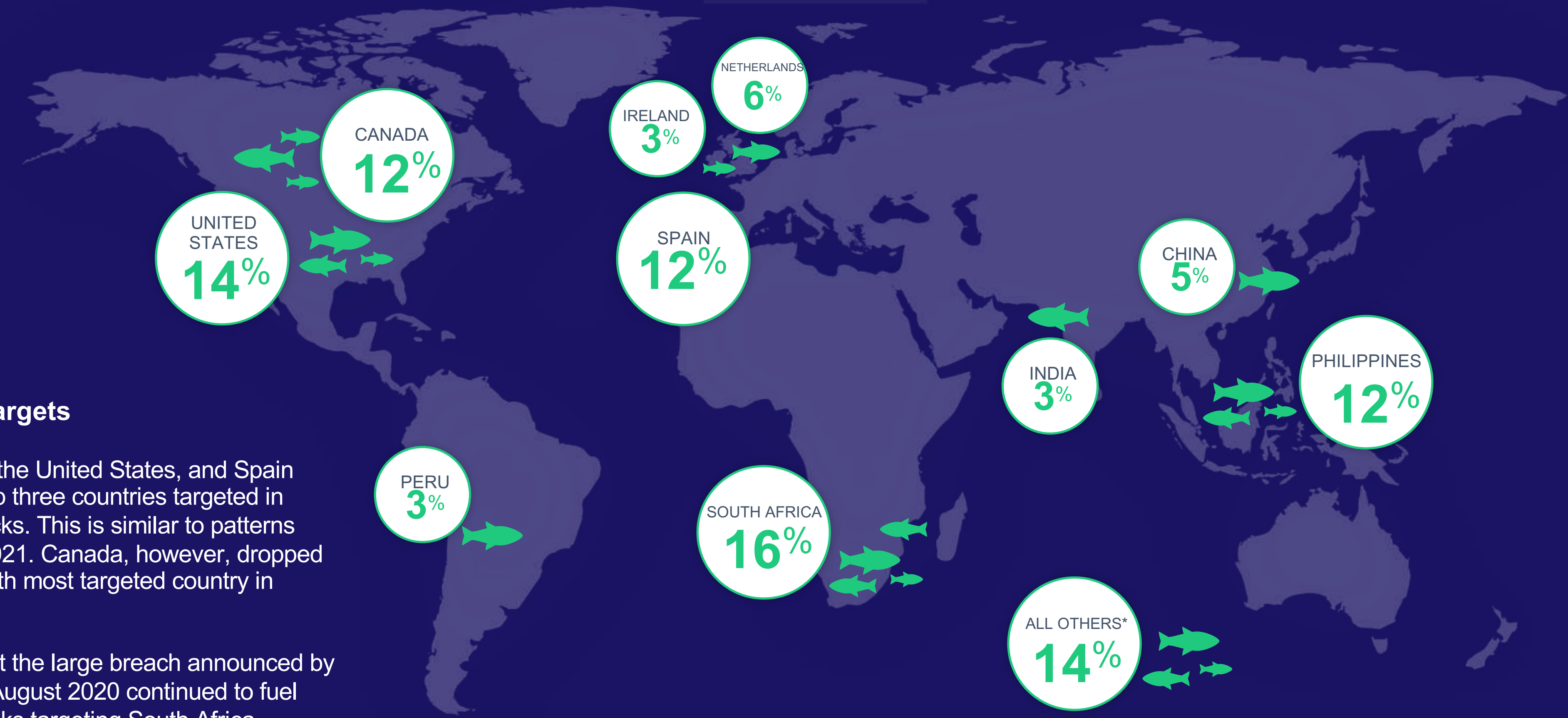
Phishing
Cyberattacks used to steal personal information from unwitting end-users under false pretenses, either by email, phone call (vishing) or SMS text (smishing).

Rogue Mobile Apps
Malicious mobile applications that exploit an organization's brand to defraud users.

Trojan Horse
Stealthy malware installed under false pretenses in order to steal personal user information.

FRAUD ATTACK TRENDS

Q2 2021 Top Phishing Target Countries



*All Others - all other countries represented <3% of total Phishing targets, respectively

Phishing Targets

South Africa, the United States, and Spain remain the top three countries targeted in phishing attacks. This is similar to patterns seen in Q1 2021. Canada, however, dropped from first to fifth most targeted country in Q2 2021.

It appears that the large breach announced by Experian[1] in August 2020 continued to fuel phishing attacks targeting South Africa.

China joined the top-10 list of targeted countries with 5% of the phishing attacks in Q2. India dropped from fifth to tenth place in our list of top-10 targeted countries; attacks targeting India dropped 47% in Q2 from Q1 this year.

Q2 2021 Top Phishing Hosting Countries

Phishing Hosts

The United States has remained the top country of origin for phishing attacks since 2017, accounting for 72.5% of ISPs hosting these types of attacks. This is largely attributable to a handful of large-scale hosting authorities~~,~~ whose sheer scale can make it easy for fraudulent activity to go undetected.

India moved from third place in Q1 to second place in Q2 as home to almost 6% of all phishing attacks worldwide. Germany dropped from second to third place in Q2, hosting over 3% of all phishing attacks.

For most of the other countries in the top 10, the percentage hosting phishing attacks is in the low single digits.

1	United States
2	India
3	Germany
4	Russia
5	France
6	Malaysia
7	United Kingdom
8	Brazil
9	Indonesia
10	Hong Kong

Compromised Cards Discovered/Recovered by Outseer

During the second quarter of 2021, Outseer recovered over 4.5 million unique compromised cards and card previews from elicit marketplaces and communications channels.

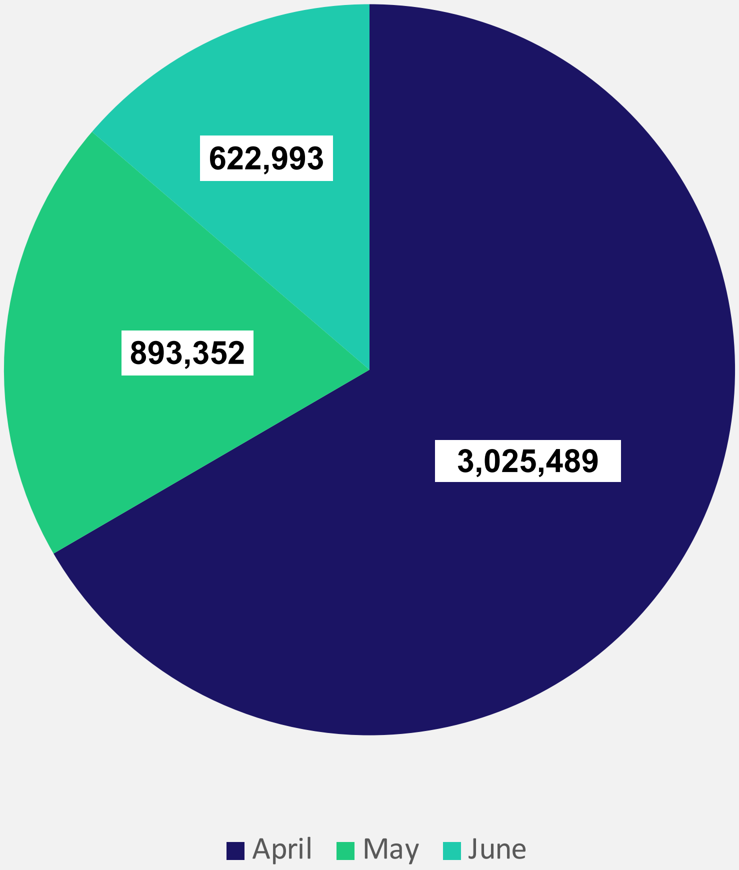
On average, Outseer recovered more than 50,000 cards a day!

The Outseer 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 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.

10 Million (H1)

Compromised cards & card previews recovered in first half of 2021

Cards Recovered by Month



Source: Outseer FraudAction Research April – June 2021

PART 2

Digital Banking & Payments Trends

Outseer researchers analyze digital banking & payments fraud trends to inform security and risk management decisions at major organizations. These efforts also serve 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 strategies across customer-facing digital channels and digital payments.

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

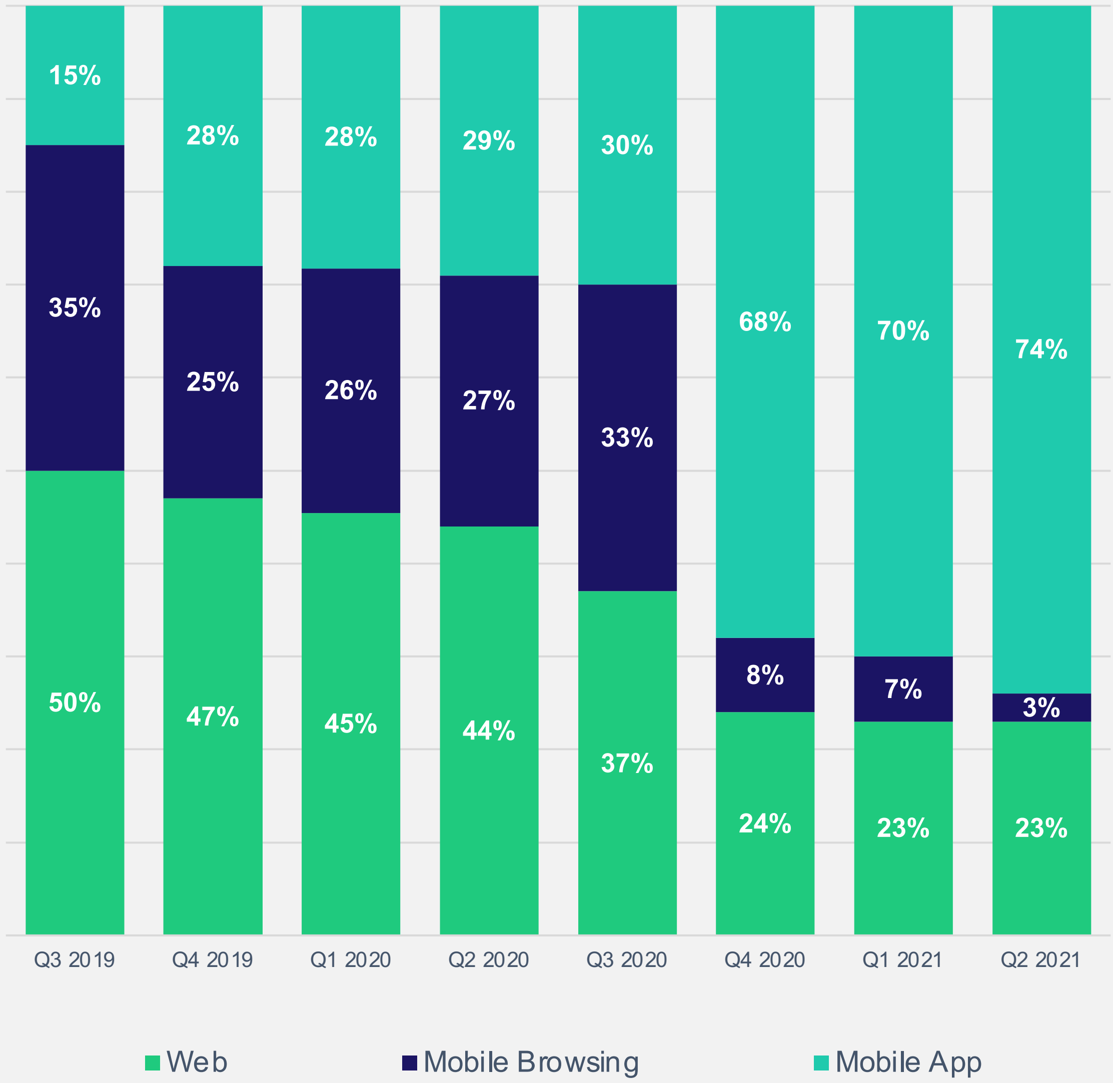
DIGITAL BANKING & PAYMENTS TRENDS

Digital Banking Transactions Distribution by Channel

Mobile banking continues to be the dominant engagement method for consumers. Today, 77% of digital banking transactions originate within the mobile channel – including mobile browsers and mobile apps. The average size of a digital banking transaction originating in the mobile channel was $550 in Q2 2021.

In contrast, the average size of transactions originating from the standard web channel was $5,700 in Q2 2021. This suggests that consumers are more comfortable performing higher value transactions from a desktop / laptop. In some cases, financial institutions may also have different transaction limits based on product, device, and/or channel.

Transaction Distribution by Digital Channel



	Q3 2019	Q4 2019	Q1 2020	Q2 2020	Q3 2020	Q4 2020	Q1 2021	Q2 2021
Mobile App	15%	28%	28%	29%	30%	68%	70%	74%
Mobile Browsing	35%	25%	26%	27%	33%	8%	7%	3%
Web	50%	47%	45%	44%	37%	24%	23%	23%

Source: Outseer Research Q3 2019-Q2 2021

DIGITAL BANKING & PAYMENTS TRENDS

Digital Banking Fraudulent Transaction Distribution by Channel

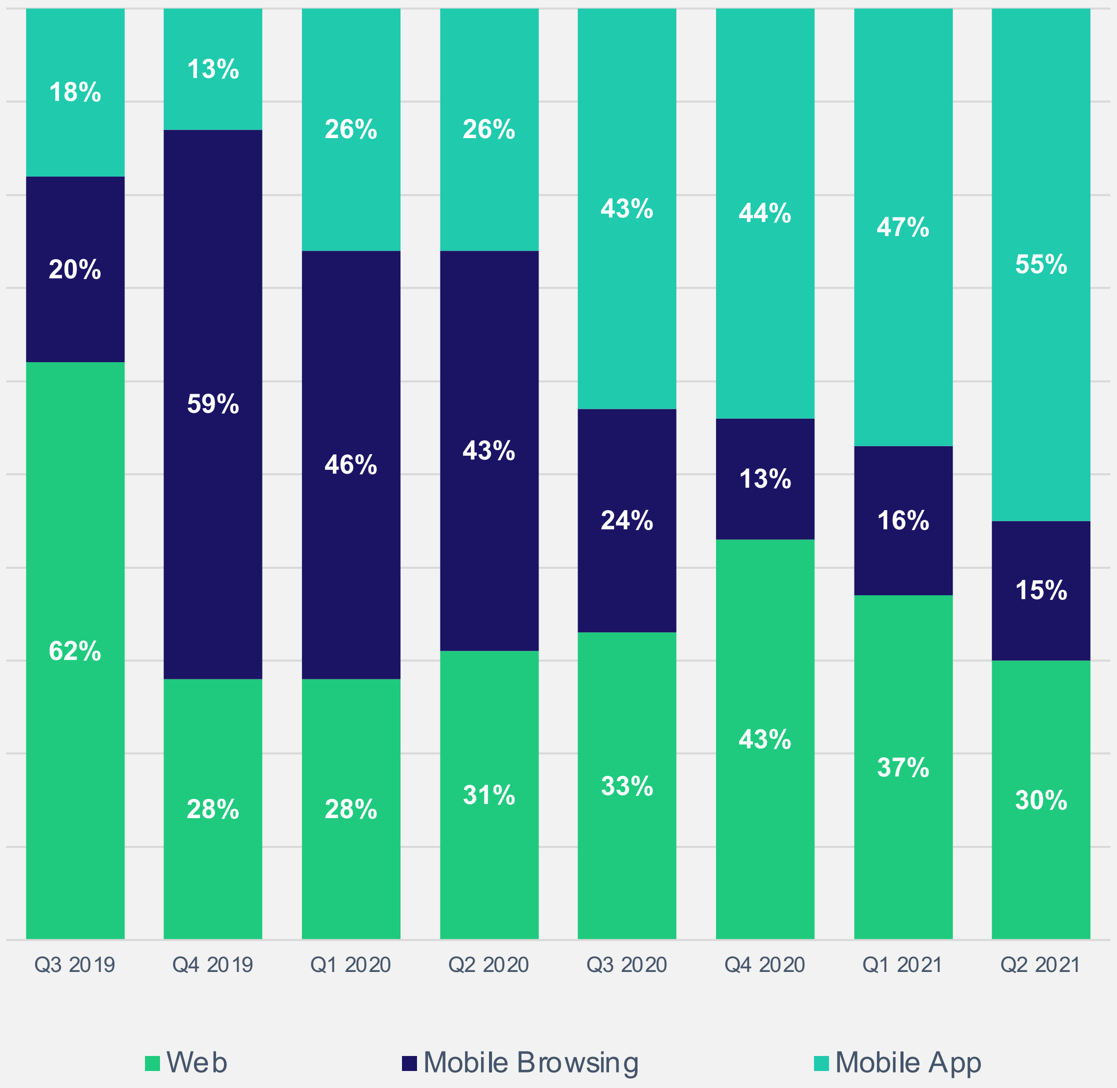
The share of fraudulent transactions originating via mobile channels continues to trend upward, growing to 70% in the second quarter of 2021 (up from 63% during the preceding three months). With consumers increasingly transacting in the mobile channel, fraudsters are quick to follow.

During the second quarter, the average value of a fraudulent online banking transaction (for example: money transfer, ACH, P2P, Wire) was $1,616 for the mobile channel and $5,158 for the web channel.

70%

of fraudulent digital banking transactions originated within the mobile channel

Fraud Transaction Distribution by Channel



Source: Outseer Research Q3 2019- Q2 2021

DIGITAL BANKING & PAYMENTS TRENDS

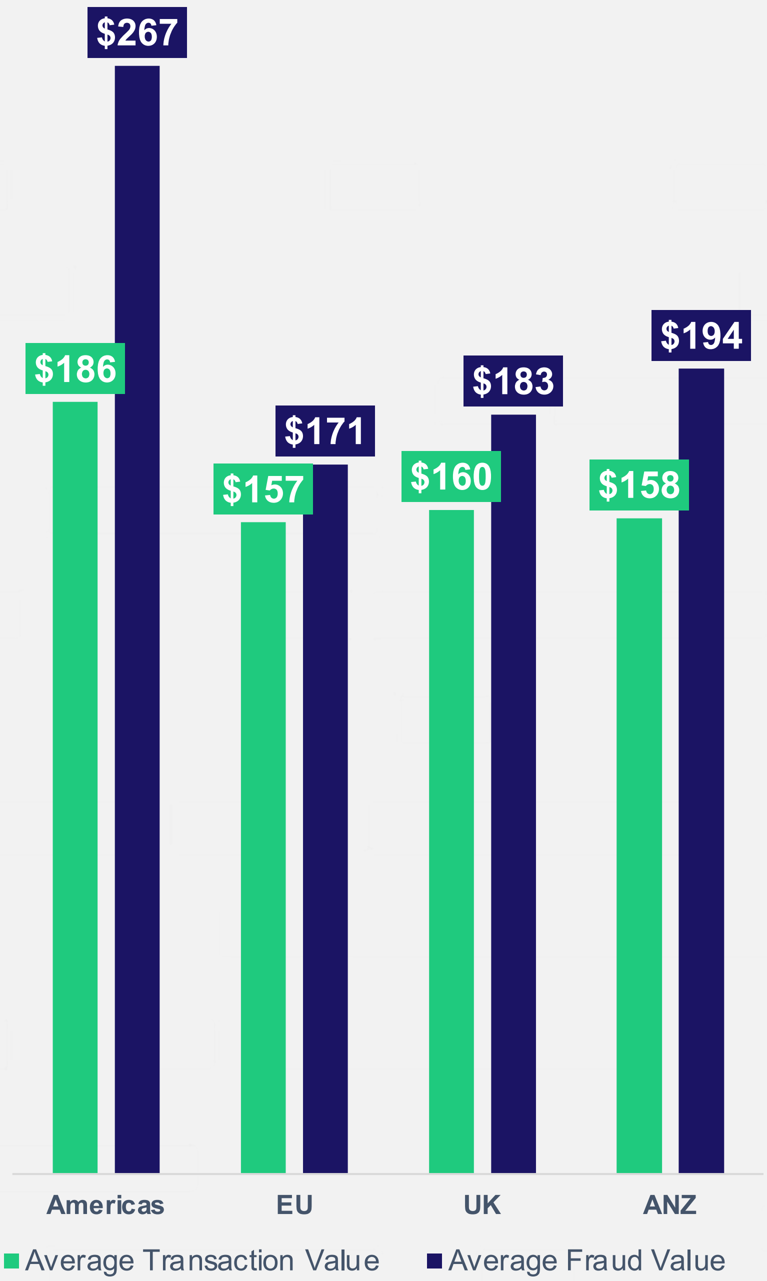
Credit Cards & Digital Payments: Average Transaction and Fraud Transaction Values

The most notable change from Q1 to Q2 this year was in Australia/New Zealand where the average fraudulent transaction value dropped over 40% from $327 in Q1 to $194 in Q2.

In the Americas, the average transaction value increased almost 18% from Q1 2021 and the average fraudulent transaction value increased 28%.

Changes in the value of transactions might be attributable to adoption of 3DS by new merchants. For example, adoption of 3DS by travel websites with high-dollar purchases might see increased averages for both legitimate and fraudulent transactions.

Average Credit Card Transaction Values



Source: Outseer Research April- June 2021

Device Age vs. Account Age

Analysis

"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.

E-Commerce

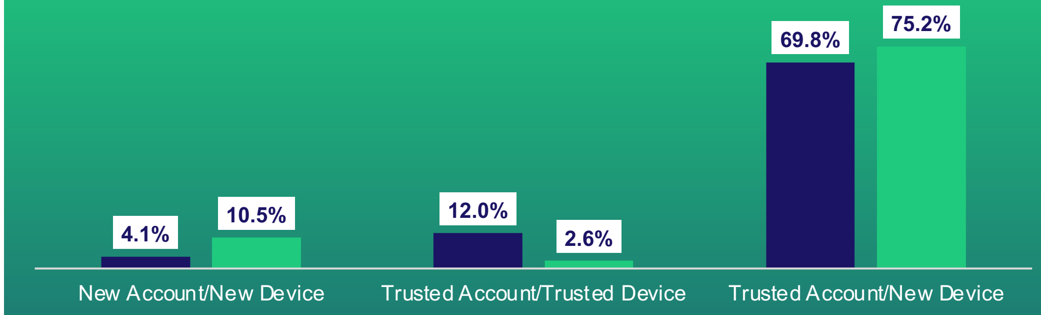
In Q2 2021, fraudulent transaction value originating from a new device and a trusted account surged 75.2% from 70.9% in Q1 2021. This is the third quarter in a row that we report an increase in this category which is reflective of the proliferation of account takeover attacks.

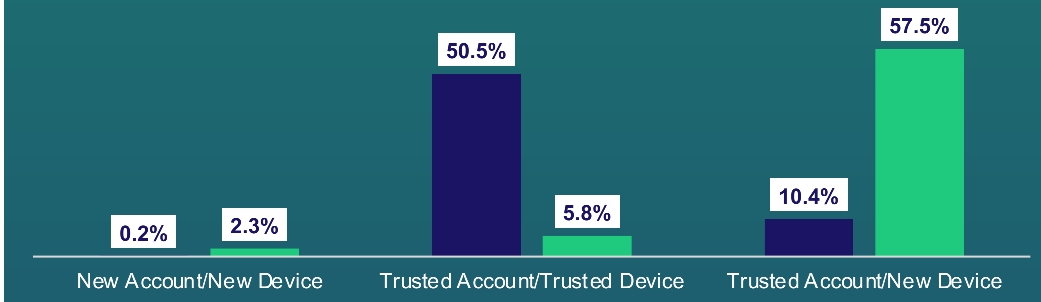
Digital Banking: Login

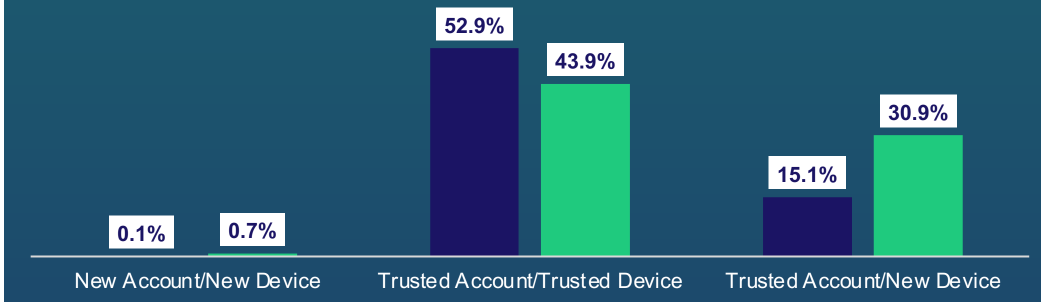
The percentage of total logins from a new device and a new account went down 33%—while the percentage of fraudulent transactions from such devices and accounts rose 35%. Meanwhile, login volumes from new devices and trusted accounts decreased from 12.2% in Q1 to 10.4% in Q2. During this same period, overall fraud decreased from 66.1% in Q1 to 57.5% in Q2 in this category showing relatively stable trend in account takeover at login. This might be a result of organizational security policies that will only take action against a suspected fraud in the event of transaction activity vs. merely logging into a trusted account. Fraud from trusted account and trusted device decreased from 9.3% in Q1 to 5.8% in Q2.

Digital Banking: Payment

Digital Banking Payment transactions from trusted devices and trusted accounts were the same in Q2 and Q1 this year (0.1%) yet fraud in this category was cut in half from 1.4% in Q1 to 0.7% in Q2 . The percentage of payment transaction volume from new devices using trusted accounts decreased from 16.9% in Q1 to 15.1% in Q2 but fraud in this category increased 52% from 20.3% in Q1 to 30.9% in Q2 reflecting the continuous growth in account takeover trend.


E-Commerce


Digital Banking Login


Digital Banking Payments

"NEW ACCOUNT": ACCOUNT AGE < 1D

"TRUSTED ACCOUNT": ACCOUNT AGE >= 90D

"NEW DEVICE": ACCOUNT-DEVICE AGE < 1D

"TRUSTED DEVICE": ACCOUNT-DEVICE AGE >= 30D

■ % of transaction volume

🟩 % of fraud value

Source: Outseer Research April- June 2021

PART 3

CNP & Digital Payments Trends

The acceleration of digital adoption stemming from the pandemic led to a surge in online transactions and digital payments. But it also introduced fraud risks that should be managed and mitigated to allow for a secure and frictionless cardholder experience.

This section includes trends in 3-D Secure Card Not Present (CNP) transactions as observed by the Outseer team.

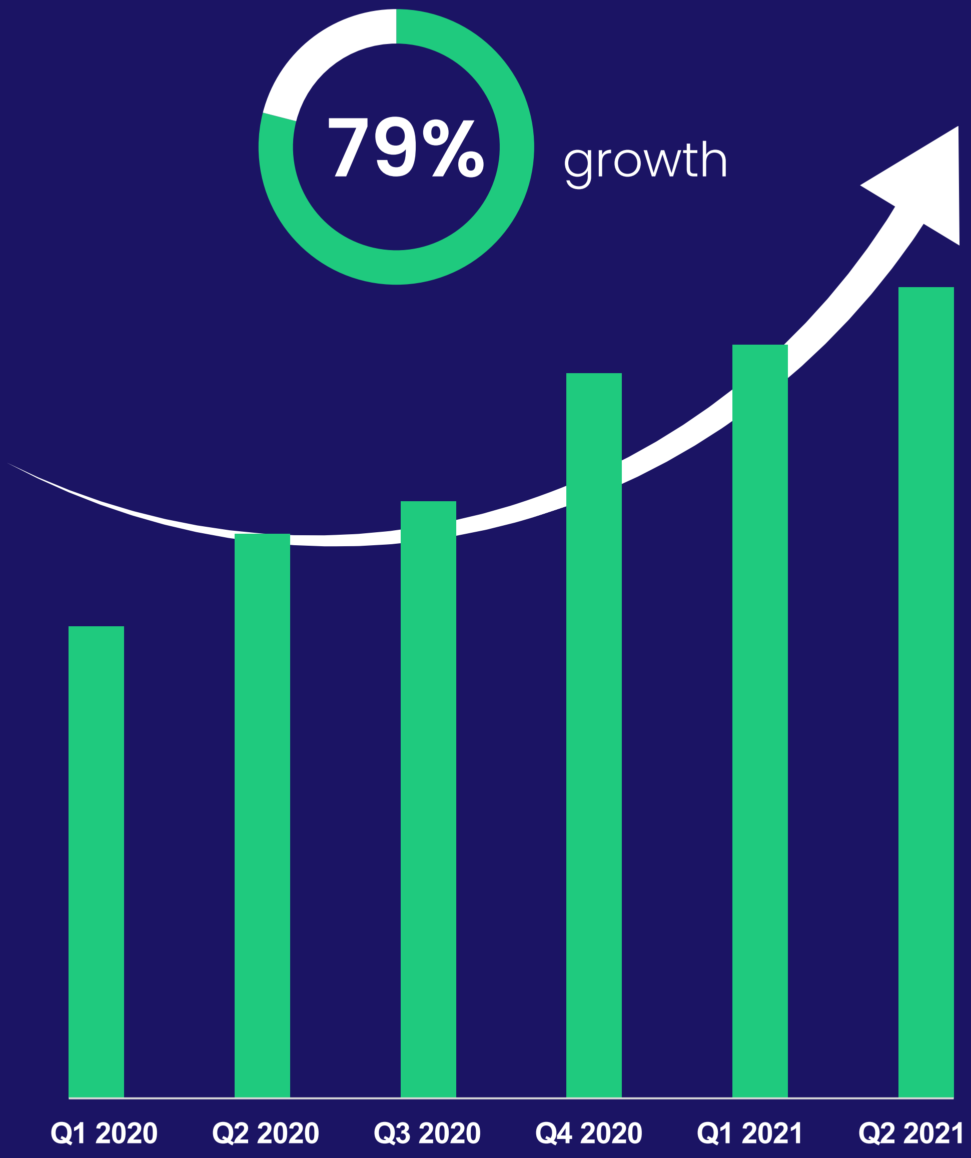
CNP & DIGITAL PAYMENTS TRENDS

3-D Secure transactions trends

Over the last 18 months Outseer has seen dramatic growth in usage of EMV® 3-D Secure (3DS) protocol, with total Outseer 3-D Secure™ transactions growing more than 79% from Q1 2020 to Q2 2021.

Our research team expects growth in Outseer 3-D Secure to continue into Q3 and Q4 2021, due to the continued transition to, and scaling of, digital payment worldwide and the upcoming holiday shopping season.

Outseer 3-D Secure™ Global Transactions



Source: Outseer Research Q1 202-Q2 2021

Global EMV® 3-D Secure (3DS) Transaction Trends

Outseer continues to observe increased growth in EMV® 3-D Secure (3DS)* transaction volumes across all geographies. Outseer saw the most significant increases in the United Kingdom (U.K.) and across the rest of Europe (EU), where EMV® 3DS' share of total 3DS transactions grew to 46% in Q2 2021. This trend is likely to continue as the PSD2 mandates for Strong Customer Authentication (SCA) drive greater acceptance and adoption of the EMV® 3-D Secure protocol.

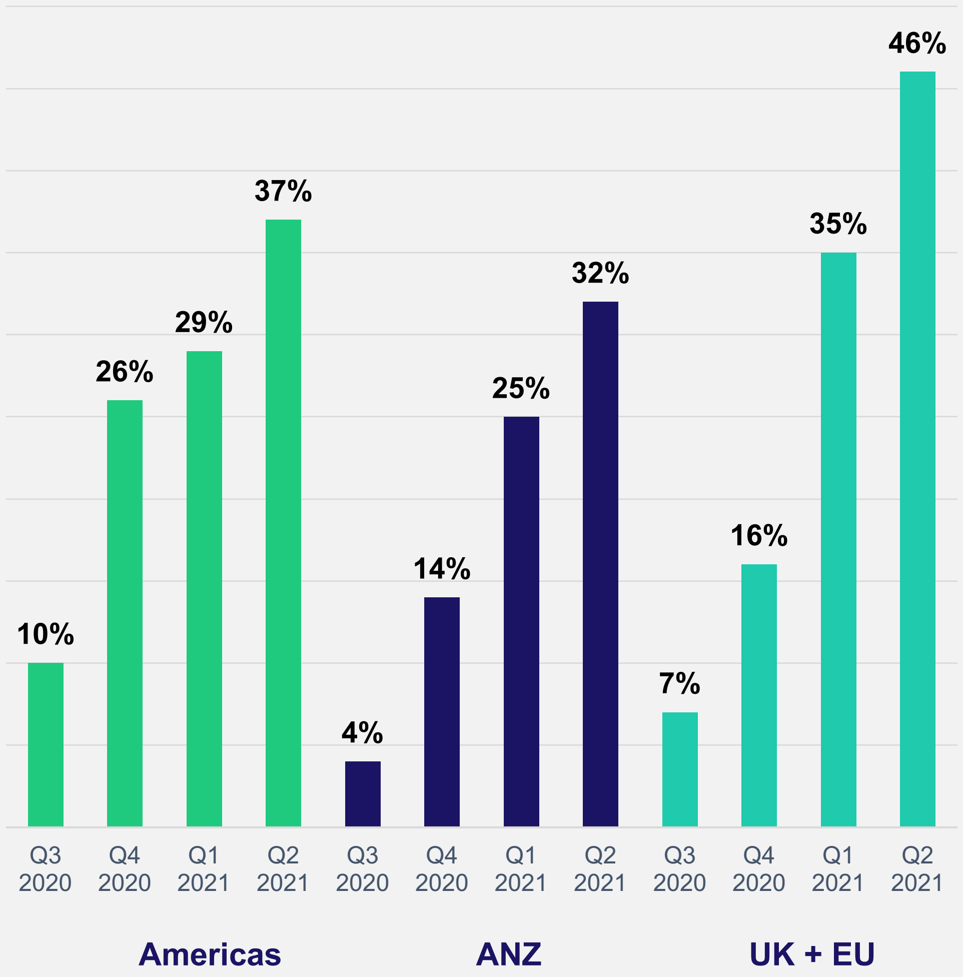
The Americas have also seen quarter-on-quarter growth in the share of 3DS-enabled transactions made using EMV® 3DS, which topped 37% in Q2 2021.Similarly, Australia / New Zealand (ANZ) have experienced similar trends in the growth of EMV® 3DS usage.

These global growth trends were likely fueled by the overall growth in CNP transactions and digital payments, as well as the migration from legacy 3DS to the latest EMV® 3DS versions.

*EMV® 3-D Secure (3DS) includes all 3DS 2.x transactions

Adoption of EMV® 3DS by merchants and card issuers helps increase transaction approval rates and drive-up revenue and profitability.

Growth of EMV® 3DS Transactions Share



Note: Represents % of total Outseer 3-D Secure transactions that are EMV® 3DS
Source: Outseer Research Q1 2020 – Q2 2021

FEATURE ARTICLE

Get Ready for Cybersecurity Awareness Month

Are you regularly interacting with your bank and communicating through digital channels? Are you using your mobile device to order ahead or to have your favorite foods delivered to your door? If the answer is “yes” to any of these questions, then you may be at heightened risk of a cyberattack.

October marks **Cybersecurity Awareness Month**, a global effort aimed at raising awareness about the importance of cybersecurity. To support this effort, the Outseer team would like to share a few best practices for protecting your organization, your customers, and yourself from financial fraud.

FEATURE ARTICLE

Get Ready for Cybersecurity Awareness Month

Fighting Fraud: Outseer Best Practices

Define your fraud and risk management strategy –
Ideally, solutions should be built to protect all digital channels and current payment types. They should also provide flexibility to support various digital commerce models such as buy online, pick up in-store (BOPIS) or buy on mobile, pick-up curbside, as well as additional new payment models as they are introduced. The best solutions will also provide-proven capabilities to detect and stop fraud – but do so in a way that maintains a seamless experience for the end user.

Employ multiple layers –
A good approach includes multiple layers to protect all of the steps in the customer journey. There is no one "foolproof" solution. Mitigate different attack vectors, such as brand abuse, phishing or rogue mobile apps, with the appropriate tools to protect your brand and your customers.

Take a risk-based approach –
For organizations executing a balanced strategy of risk and experience, protect your transactions with risk-based authentication. One of the significant improvements in the latest EMV® 3-D Secure protocol is the incorporation of a risk-based approach – one that Outseer has been pioneering for over a decade. This allows legitimate cardholders to transact without interruption and improves cardholder trust and loyalty.

For those few, higher risk transactions that require additional verification, use strong step-up authentication options. It is also recommended to use dynamic data elements so that in the event data is compromised, it is rendered useless for future transactions.

Raise universal awareness –
As fraudsters evolve their strategies, it is important to educate your customers, employees, and business partners on the latest potential threats and what types of scams to look out for. It is particularly important to be aware of fraudsters' attempts to manipulate daily communications, messaging, and other digital interactions.

Promote shared responsibility –
Fighting fraud as a community will help contribute to faster and more accurate fraud detection and prevention. Outseer introduced the Outseer Global Data Network^{TM} over a decade ago – the first global consortium of fraud and transaction data, with thousands of contributors worldwide.

Developing a plan to address these steps will help you, your customers, and your organization fight fraud. If you would like to receive more information or discuss strategies on how to implement best practices to protect your customers and organization against fraud, please contact the Outseer Team at:

https://www.outseer.com/contact-us/

Do Your Part. #BeCyberSmart

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, 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.

www.outseer.com

[1] Experian “Experian Data Breach”