# ONLINE PAYMENT FRAUD

Emerging Threats • Segment Analysis • Market Forecasts • 2021-2025

Reprint for Experian

www.juniperresearch.com

JUNIPER RESEARCH

First Published April 2021

Published by:
Juniper Research Limited,
9 Cedarwood,
Chineham Park,
Basingstoke,
RG24 8WD, UK
UK: Tel +44 (0) 1256 830001/475656
US: Tel +1 408 716 5483
www.juniperresearch.com
info@juniperresearch.com

Printed in United Kingdom

Nick Maynard and Susan Morrow are the Authors of this Work

## Report Author

Nick Maynard and Susan Morrow

Juniper Research endeavours to provide accurate information. Whilst information, advice or comment is believed to be correct at the time of publication, Juniper Research cannot accept any responsibility for its completeness or accuracy. Accordingly, Juniper Research, author or distributor shall not be liable to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by what is contained in or left out of this publication.

This report contains projections and other forward-looking statements that have been developed through assumptions based on currently available information. All such statements and assumptions are subject to certain risks and uncertainties that could cause actual market parameters and performance to differ materially from those described in the forward-looking statements in the published reports. Such factors include, without limitation, unanticipated technological, environmental, political, social and economic factors beyond the control of Juniper Research.

Forecasting is by definition a dynamic process that depends on the factors outlined above and can be vulnerable to major changes as a result. Juniper Research operates a policy of continuous improvement and reserves the right to revise forecasts at any time without notice.

If you wish to quote Juniper Research please submit the planned quotation to info@juniperresearch.com for approval.

# Foreword

## Juniper Research Limited

Juniper Research is a European based provider of business intelligence. We specialise in providing high quality data and fully-researched analysis to manufacturers, financiers, developers and service/content providers across the communications sector.

Consultancy Services: Juniper Research is fully independent and able to provide unbiased and reliable assessments of markets, technologies and industry players. Our team is drawn from experienced senior managers with proven track records in each of their specialist fields.

## Regional Definitions

| | |
|---|---|
| North America: | Canada, US. |
| Latin America: | Argentina, Aruba, Bahamas, Barbados, Belize, Bolivia, Brazil, Cayman Islands, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, French Guiana, Grenada, Guadeloupe, Guatemala, Guyana, Haiti, Honduras, Jamaica, Martinique, Mexico, Netherlands Antilles, Nicaragua, Panama, Paraguay, Peru, Puerto Rico, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Surinam, Trinidad and Tobago, Turks and Caicos Islands, Uruguay, Venezuela, Virgin Islands. |
| West Europe: | Austria, Belgium, Cyprus, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, UK. |
| Central & East Europe: | Albania, Belarus, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Moldova, Montenegro, North Macedonia, Poland, Romania, Russia, Serbia, Slovakia, Slovenia, Turkey, Ukraine. |
| Far East & China: | China, Hong Kong, Japan, Macao, South Korea, Taiwan. |
| Indian Subcontinent: | Bangladesh, India, Nepal, Pakistan, Sri Lanka. |
| Rest of Asia Pacific: | Australia, Brunei, Fiji, New Caledonia, New Zealand, Cambodia, Indonesia, Laos, Malaysia, Maldives, Mongolia, Myanmar, Philippines, Singapore, Thailand, Vietnam. |
| Africa & Middle East: | Afghanistan, Algeria, Angola, Armenia, Azerbaijan, Bahrain, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo, Cote d'Ivoire, Democratic Republic of Congo, Djibouti, Egypt, Equatorial Guinea, Eswatini, Ethiopia, Gabon, Gambia, Georgia, Ghana, Guinea, Guinea-Bissau, Iran, Iraq, Israel, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Lebanon, Lesotho, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Oman, Palestine, Qatar, Reunion, Rwanda, Saudi Arabia, Senegal, Seychelles, Sierra Leone, South Africa, South Sudan, Sudan, Syria, Tajikistan, Tanzania, Tunisia, Turkmenistan, Uganda, United Arab Emirates, Uzbekistan, Yemen, Zambia, Zimbabwe |

## Contents

< >

# 1. Online Payment Fraud: Market Overview

## 1.1 Introduction

Digital payments, already a booming industry before the COVID-19 pandemic, have since been a key part of a social distancing strategy used by governments in the world. Since the pandemic, record numbers of online payments are being processed on all channels, but especially digital. Juniper Research forecasts that wallet users will exceed 4.4 billion globally in 2025, from 2.6 billion in 2020.

From market data it is clear that online payment is convenient and drives eCommerce. However, it has also created a playground for cybercriminals intent on circumventing the structures on which online payments rely. Trust, it seems, is breaking down. A 2021 report from Experian that looks at global fraud, points out a systemic issue in how fraud is being handled.

Organisations' seemingly misplaced confidence in their ability to identify and re-recognise customers is contributing to higher fraud losses and a subsequent lack of trust.'[i]

This finding leads to the idea of establishing 'zero trust' payment ecosystems that offer an option to always verify, never trust or store, with security measures, including tokenisation, providing the backbone to achieve this.

The threat landscape continues to evolve and test existing anti-fraud measures. The omnichannel retail environment, fuelled by changing customer expectations, restrictions during the pandemic, along with initiatives that are encouraging the open use of financial data, are creating a perfect storm for fraud. Fresh and upgraded challenges must be tackled in the world of online payments. New types of fraud such as 'silent fraud' and cybersecurity vulnerabilities are all contributing to a complex mix of attack vectors.

As in any other industry, disruption has the potential to be a force for good; it opens up opportunities through innovation. However, online payments are not isolated, they operate in a complex web of interactions and the use of open APIs (Application Programming Interfaces), whilst creating expansive opportunities for all stakeholders, must now be a consideration. The identity network, a key component of payments, is also a driving force that, used well, can build trust, but also adds into this heady mix of opportunities for fraud.

Cybercriminals are always one step ahead. They use a mix of social engineering and technology know-how to circumvent systems. Fraudsters' ultimate aim is financial, so payment systems are the ideal target. Juniper Research estimates that there was a $27 billion eCommerce transaction fraud loss in 2020 and that this will reach over $52 billion in 2025, as the eCommerce ecosystem expands.

Understanding the threat landscape is crucial to reinforcing protections, whilst keeping innovation clear of exploitation.

## 1.2 Types of Fraud

Fraudsters are highly innovative and use whatever means available to intercept, manipulate, and misrepresent financial transactions for personal financial gain.

Identity is sitting as a central pivot in the payment ecosystem for both customer engagement and fraud prevention. As identity has become intrinsically entwined with payments, the focus of the fraudster has been innovating around identity or more precisely, identity data. Methods of fraud reflect new technologies and new processes. The fraudsters toolkit does not only become ever-more sophisticated, but it expands its range and scope of attack. Attacks are often multi-part, drawing in the social as well as the technical to execute a fraud event. The following is a list of the top fraud attack methods:

- Identity fraud and KYC (synthetic identity) – the data that describes an individual is an inherent part of the payment's ecosystem. The assurance that a payment transaction is checked using a robust KYC/CDD (Know your Customer/Customer Due Diligence) process is vital in reducing fraud. However, ever-more sophisticated synthetic identity fraud is changing the metrics of KYC/CDD. Technologies such as deep fakes will be used to confuse the KYC process; making it vulnerable to deep fake identities and making fraudulent events harder to detect.

- Silent Fraud – keeping under the radar is a tactic used in other cybercriminal techniques, for example, in detection evasion by malware. It makes sense that fraudsters will use detection evasion in fraudulent activity around payments. In this type of fraud, small amounts are taken from thousands of accounts – the whole adding up to often more than a single large fraud event. A report from the RUSI (Royal United Services Institute) has termed this threat the 'Silent Threat' and positioned fraud as now being more about defrauding at the individual level than at the bank level. The report states: 'While the 'hidden' nature of the crime makes assessing the true volume and cost of fraud against individuals difficult, it is clear from available statistics that the scale of the problem is vast, with one report from 2017 suggesting that fraud against individuals was at that time as high as £6.8 billion ($9.4 billion).'[ii]

- Clean Fraud – is a transaction that passes a merchant's typical checks and appears to be legitimate, yet it is actually fraudulent. For example, the order has valid customer account information, an IP (Internet Protocol) address that matches the billing address, accurate AVS (Address Verification Service) data and card verification number, etc. (i.e. the fraudster has managed to steal every piece of data required to carry out a purchase).

  Clean fraud is very difficult to combat because there are seemingly no anomalies to detect. The only options are either to ask more questions, which introduces friction to the buying process; or, to passively leverage increasingly richer data about the context of the transaction or the digital behavioural signals from the interaction.

- Account Takeover – is a type of identity fraud where criminals attempt to gain access to a consumer's funds by adding their information to the account (for example, adding their name as a registered user to the account, changing an email or physical address).

- Friendly Fraud – occurs when a merchant receives a chargeback because the cardholder denies making the purchase or receiving the order, yet the goods or services were actually received. In some instances, the order may have been placed by a family member or friend that has access to the buyer's cardholder information.

- Chargeback Fraud – similar to friendly fraud, as a chargeback request is made in spite of received goods and services. While friendly fraud is non-malicious in nature, chargeback fraud is typically a premeditated intention to commit fraud.
- Affiliate Fraud – this type of fraud involves the fraudulent use of a company's lead or referral programmes to make a profit. For example, companies may submit phoney leads with real customer information, or inflate web traffic to increase their payout before the merchant is aware of the scam.
- Re-shipping – this typically involves fraudsters recruiting an innocent person (known as a 'mule') to package and re-ship merchandise purchased with stolen credit cards. Since the mule has a legitimate shipping address, the merchant would have no reason to suspect fraud. The fraudsters then ask the unsuspecting individual to re-package and send the goods to them.
- Botnets – a botnet is a network of infected machines controlled by a fraudster (the 'botmaster') to perpetuate a host of crimes. In the case of eCommerce, the infected device could be used with stolen payment and identity information, so the transaction appears to originate from a location that reasonably matches the credit card in use. In this way, infected computers appear to be 'good' when, in fact, they are not.
- Phishing – is the practice of sending seemingly official emails from legitimate businesses to steal sensitive personal information from customers, such as account login details, passwords and account numbers.

A variation of phishing is SMS phishing (or smishing) where a fraudster sends a text message that asks a mobile phone user to provide personal information, such as their online banking password, or asks the phone user to make a phone call to a number controlled by the fraudster and then enter their ATM PIN number or online password.

Phishing has increased drastically during the pandemic. Reports have shown increases of staggering amounts, a CGI survey showing an increase of 30,000% in threats related to COVID-19.[iii] Google admitted to blocking 18 million coronavirus related emails per day in April 2020.[iv]

- Whaling – is a variation of phishing, but targets or 'spears' a specific subset of consumers, customers or employees. Fraudsters send tailored messages that appear to have come from the targeted entity's organisation, sent by another staff member, known business partner or other trusted party. BEC (Business Email Compromise), a form of whaling, has seen increases in 2020 with an 81% increase between Q2 and Q3 of 2020, according to reports observing BEC related scams.[v]
- Pharming – re-directs website traffic to an illegal site where customers unknowingly enter their personal data.
- Triangulation – this enables fraudsters to steal credit card information from valid customers, typically through online auctions, ticketing sites, or online classified ads. A fraudster posts a product online at a severely discounted price, which is purchased by a customer using a valid credit card. The fraudster uses other stolen payment credentials to purchase and ship the product from a legitimate website to the customer. Neither the merchant nor the customer suspects anything, yet both have been duped. In the meantime, the fraudster now has access to the

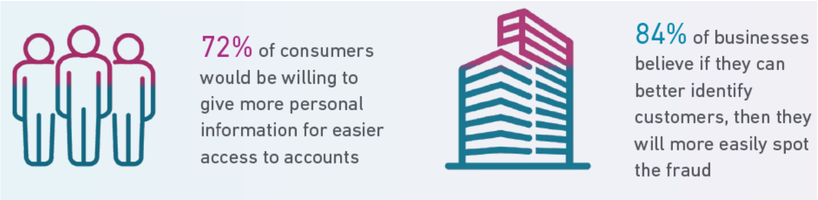
unsuspecting buyer’s card number and can continue to steal and amass other credit card numbers using the same scheme.

- Pagejacking – based on the copying of a legitimate website and using it to spoof customers to take payments. It is often associated with malicious SEO (Search Engine Optimization) campaigns. Client-side attacks against content management systems of websites can lead to this type of fraud.
- Online payment services are rapidly moving to, or are already active in, ecosystems of interrelated players and connected systems (including apps and APIs). The increase in digital payments as a reaction to social distancing during the pandemic has been like a red rag to a bull in terms of cyber-targeting by fraudsters. A report on the US digital economy by Adobe shows a spend of $190 billion via smartphones during 2020, which are expected to contribute to 50% of all online spend by 2022.[vi] Even with the pandemic restrictions, contactless payments are still heavily geographic. Overall, however, Mastercard found that in 2020 F2F contactless payments grew 25% compared to 2019.[vii]

## 1.3 Key Trends in Digital Fraud

It is not surprising that as eCommerce transactions grow year-on-year, so do the number of fraudulent transactions.

**Figure 1.1: Experian Fraud Statistics**



72% of consumers would be willing to give more personal information for easier access to accounts

84% of businesses believe if they can better identify customers, then they will more easily spot the fraud

*Source: Experian*

According to the Experian 2020 Global Identity and Fraud Report, 57% of businesses are reporting higher losses associated with account opening and account takeover fraud in the past 12 months, compared to 55% in 2018 and 51% in 2017.

The payment’s ecosystem is improving customer experience but developing fraud access through new sources of payment pathways and greater access to human touchpoints. The human in the payments’ machine is increasingly a target, but achieving a balance between human needs and security remains a top priority. The mechanics of out of band payment journeys adds complexity to this. Experian’s view of ‘digital takeaway fraud’ is that businesses need to ensure that any disconnect across the ecosystem, such as when customers buy online and pick up later, are covered by anti-fraud technologies and processes.

This section will look at the biggest trends in the online payment fraud area.

## 1.3.1 Fitting the Human into Payment Fraud

The human in the payments' machine is a key trend in payments and informs the entire ecosystem mechanics from usability to anti-fraud. The overlap in creating great customer experiences in payments and matching these to a secure experience is perhaps the greatest challenge of the industry. Balancing security measures vs usability has always been a difficult objective across many sectors, but this goal is heightened by the focus of cybercrime on the payment sector. CNP (Card Not Present) fraud at 34% and account takeover at 24% are major fraud threats for merchants. And, staggeringly, 86% of global consumers fall foul of payment fraud and ID theft.[viii]

Account takeover must be a focus, as account control can have long-reaching problems; a survey by TransUnion (iovation) of 1,068 adult Americans found a 347% increase in account takeover and 391% rise in shipping fraud attempts globally.[ix]

The pandemic is exacerbating identity theft issues. A recent US report found a spike in unemployment clams during the pandemic, with an associated increase in stolen PII (Personal Identifiable Information). The FBI is calling for better identity verification to prevent identity-related fraud.

A 2020 report from the EU Payment Council places emphasis on elements that make full use of personal data and identity to create tactical cybercrime:

- Social engineering
- Malware
- APTs (Advanced Persistent Threats)
- Denial of service
- Botnets
- Monetisation channels

The report goes on to say that:

'Concerning card payment fraud, criminals are changing their approach. Not only by changing to more high-tech frauds like APT, but also a part of the criminals is reverting to old school types of fraud such as lost and stolen, sometimes in combination with social engineering. As e-commerce is still on the rise, CNP fraud remains a significant factor for fraud losses.'

Anti-fraud techniques must work to minimise friction whilst maximising detection capability. This must be done across multiple channels with no gaps. The multiple parts of a payment model across all the human touchpoints means that the many moving parts of the system must be oiled by anti-fraud and fluid identity verification. The emergence of identity networks that can handle multiple sources of data and verification services will help move the scales towards a more balanced security-usability model.

However, what cannot be forgotten is that even with the best structures in place, cybercriminals continue to test the waters by using a mix of social and technical to circumvent exceptional anti-fraud measures. The human in the middle of the payment lifecycle must always take centre stage and clever measures to ensure customers are not tricked should be part of a wider anti-fraud programme.

### 1.3.2 Continued Darknet Activity & Messaging Apps

#### i. From Darknet to Clearnet

Dark web sites that sell stolen identity data are here for the long haul. Unfortunately, as one dark web marketplace is closed down, another one pops up. The dark web continues to be used as a conduit to deliver the documents of cybercrime, including forged ID docs, stolen ID data and credentials, spoof pages, bank Trojans, etc. Researchers at PrivacyAffairs look at the prices of various illegitimate items for sale via dark web marketplaces in their 'Dark Web Price Index.' The 2021 edition shows costs of credit card data, payment processing services, and forged documents. A PayPal transfer from a stolen account, $1,000 – $3,000 is valued at $320.39, whereas an average-quality US driving licence goes for $70. A cloned credit card with $1,000 account balance is only $12.[x]

The darknet itself is part of a wider ecosystem incorporating the services of apps like Signal, Telegram, and WhatsApp. Research from Motherboard found a Telegram bot being used to sell phone numbers of Facebook users that were part of a Facebook data breach impacting over 500 million users in 2019. This widening of the ecosystem is part of a move to automate the business of cybercrime and one that should be part of any strategic security posture within the payment's sector.

#### ii. Key Takeaways

Diversification and convenience are watchwords for the fraudster community. In 2020, 37 billion data records were breached.[xi] This provides all the materials needed to perpetuate fraud on a massive scale. Identity theft, synthetic identity, social engineering and other scam tools are built upon the data that payments rely on to be true. The cybercrime ecosystem is now complete with every trick in the book being used. From the dark web to apps, the cybercrime communication network is hardened and working. Counterbalancing this with anti-fraud also requires an ecosystem approach. No part of the whole can be left unattended. From the delivery of friction-reduced verification to ML-enabled AML (Anti Money Laundering) checks, no anti-fraud stone can be left unturned.

The result is that FDP (Fraud Detection and Prevention) spend must be as broad as possible, as the potential attack vectors cover 360-degrees. FDP vendors must be as actively engaged as possible in understanding new fraud methods to counter the high level of innovation in this area.

Dark markets typically encourage the use of strong encryption tools for sensitive communications, while it is difficult to discover the location of so-called 'onion' (hidden service) servers. This means that while the authorities may be able to discover the identity of dark market customers following their use of tools bought illicitly, vendors are hidden behind an additional layer of protection. This, and the fact that dark market tools can be sold to any customer wishing to commit fraud, means that the origin of any tools developed can be difficult to pin down in terms of their location, assuming there are no giveaways in supplied code or documentation. And as the authorities close one marketplace, another appears to replace it. The security industry must never feel as if it can sit on its laurels, as cybercriminals are the masters of reinvention.

The 'as-a-service' business side of hacking continues to deliver the tools of fraud at a cheap price, we should expect the market for PII to explode, as opportunities to exploit identity continue. The following tables from Flashpoint gives the average list price for various exploit kits on major darknet markets; a tailored phishing page can be purchased for around

$35. Costs for these services are decreasing as availability and the market increases. Payment card data is also dropping in price.

The use of the dark web in the fraud space makes it difficult for FDP vendors to correctly engage with, and counter, new and emerging threats. It also makes it easy for relatively unskilled actors to use available tools to commit ever increasing fraud levels.

In order to combat this, FDP vendors must both invest in research to understand the latest attack traders being exposed using dark web tools, as well as co-ordinate with authorities to ensure that actions are being carried out in a comprehensive way. As more tools come online that can perform deep analysis of darknet websites, vendors should also look to see if integration with these tools can enhance their own anti-fraud measures.

### 1.3.3 Identity Theft

Consumer-focused online transactions (including those carrying payments) are based on having verified consumer identity. Because of this, identity data is a prime target for fraudsters. In the US, the Consumer Sentinel Network, part of the FTC (Federal Trade Commission), tracks identity-related fraud. In 2020, Sentinel received more than 2.1 million reports of fraud, with consumers losing $3.3 billion to fraud in 2020.[xii] The report highlights that there were 1.4 million reports of identity theft. In 2020, 406,375 reports were associated with misused PII used to apply for a government document or benefit – the figure in 2019 was only 23,213. In the UK, CIFAS warned of fraud spikes of 90% in 2020 and 2021 with the majority of people being unprepared for this.[xiii] Online verification of identity during a transaction has several flavours. The use of verification can be both as a persistent assurance level, as offered by various government ID schemes, or as an on-the-fly check as offered using ID Networks and data orchestration-based services (such as offered by Thales). eWallet type systems, including potentially self-sovereign, may also offer verified claims that could be used to definitively identify a user. The Open Banking initiative also has massive potential to be used to assure a user (as well as manage the payment) during an online transaction. More sensitive or important resources like online banking and other financial accounts require high levels of user identity and anti-fraud checks. Proof of identification and often intensive online KYC processes are becoming a fundamental need in the payment industry, but can lead to excessive friction and customer abandonment – ultimately leading to lost sales. In a recent interview by Finextra TV, Tony McLaughlin, Emerging Payments & Business Development at Citi, summed up the situation: ‘If we fix identity, we fix payments.’[xvi]

The other end of the identity spectrum is the focus of cybercrime on manipulating human behaviour via techniques like spear-phishing. Social engineering is highly effective, and during the COVID-19 pandemic, phishing spikes were observed by many security vendors.

KYC checks are also falling short: In 2020 major fines were issued to FIs across the world for AML/KYC and other regulation violations.[xiv] KYC checks are costly and can impact negatively on the user experience. It can take between 90-120 days to onboard corporate banking customers, for example. In terms of meeting KYC requirements for compliance, a large FI requires 307 employees to work on meeting the standards.[xv]

As APIs increasingly become part of the identity ecosystem and by association, the payments ecosystem, securing the API system must become a central aspect of a 360-degreee angle on generating a secure payments ecosystem posture. The Akamai 2020 State of the Internet report states that ‘attackers often target REST and SOAP endpoints that provide access to confidential data and services that bad actors can use to commit financial crimes.’ API credential stuffing attacks  are an important aspect of securing the payments ecosystem, with Akamai stating that attacks against APIs have grown in recent months and at times account for 75% of attacks. Deepfakes and identity is a concern for 77% of cybersecurity decision makers in the financial sector, according to a report by iProov.[xx] The report also found that around 50% of respondents believed deepfakes were a high risk for online payments.

Synthetic identity is where a cybercriminal uses snippets of legitimate data (like a Social Security Number) then adds in other made-up data to create a synthetic identity. They then use this ID to commit fraud, including apply for loans, set up lines of credit, etc. The Federal Reserve Insights for July 2020 found that the rates of approved accounts at financial institutions to be issued to a synthetic identity could be as high as 2.7% of all new accounts.[xvi] An ID analytics study from Lexis Nexis found that only half of synthetic fraudsters apply for credit using digital channels. This allows the assumption that a significant number of fraudsters can pass KYC tests even when appearing in person.

‘Traditional fraud models are not designed to detect synthetic identities,’ said the Boston Fed; citing research that showed such models were ineffective at catching 85% to 95% of likely synthetic identities.[xvii]

### i. Data Breaches

Data breach volume and rates continue to rise; figures from Risk Based Security show data breaches reaching a record 37 billion in 2020. A substantial proportion of these breached data records contain sensitive personal or credential information that can be used as part of attempts to carry out fraud on a number of sites or services. Data breaches are themselves a pathway to further crime. Credential stuffing is one such follow-on activity; this is where previously exposed login credentials are used to facilitate account takeover. Akamai identified 100 billion credential stuffing attacks from July 2018 to June 2020, 10 billion targeting the gaming industry. COVID-19 and remote working have played a large part in credential theft, with phishing at an all-time high.

An avalanche of stolen data is providing a continued playground for current and future account takeover; leading to other crimes, including synthetic ID and KYC fraud, that increase the success of fraudulent events against payments. Authentication options such as risk-based biometrics can offer a hope in the future of payment authentication. Juniper Research found that biometrics will authenticate over $3 trillion of payment transactions in 2025, up from $404 billion in 2020. However, KYC is critical in payments and attention to verification to avoid synthetic identity is one part of a highly complex jigsaw puzzle. There appears to have been little let-up in the number and size of data breaches occurring year-on-year. There have already been a number of significant breaches in 2020, as shown in the following table:

## Figure 1.2: Significant 2020 Data Breaches

| Brand | Date | Impact |
|---|---|---|
| Greek tourist services portal | January 2020 | Greece's four main banks – Alpha Bank, Piraeus Bank, Eurobank and the National Bank of Greece cancelled 15,000 credit and debit cards after payment card data was hacked. |
| Antheus Tecnologia | March 2020 | Biometric data breach – 76,000 fingerprints exposed. |
| Nintendo | April 2020 | Nintendo – credential stuffing - 160,000 accounts affected. |
| Zoom | April 2020 | 500,000 Zoom passwords for sale on the dark web – multiple security vulnerabilities. |
| Facebook | April 2020 | Over 267 million Facebook profiles found listed for sale on the dark web. |
| EasyJet | May 2020 | 9 million customers' personal data – breach details unknown. |
| Dave (mobile banking app) | July 2020 | Third-party breach - account details of over 7.5 million users exposed. |
| FireEye (large security firm) | November 2020 | Unauthorised third-party actor accessed FireEye networks and stole |

*Source: Juniper Research*

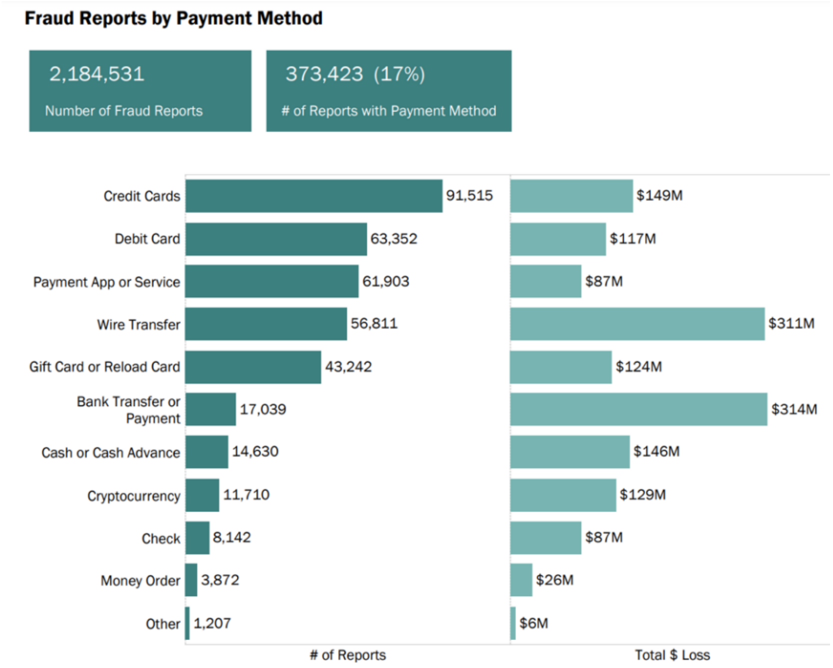
Cybercrime is being enabled by a mix of techniques and tactics. Multi-part cyber threats show that cybercriminals will use every trick in the book.

Whilst phishing is key in data breach events, misconfiguration and accidental exposure should not be overlooked. The 2020 Verizon DBIR (Data Breach Investigations Report) found 43% of all data breaches targeted web applications. During 2020, a noticeable increase in misconfigurations of web apps, servers, and other components, lead to exploitable vulnerabilities.[xviii] A 2020 survey of cloud engineering and security teams found that 73% of respondents experience more than ten incidents a day.[xix]

Importantly, as banking APIs become more advanced and widely used, API security issues are likely to become a higher profile part of the threat landscape. The Open Banking movement is beginning to find its feet and, in the UK, 2.5 million consumers and businesses use Open Banking-enabled products. Open Banking is also being used as part of ID Networks to verify users, basing the results on already KYC checked personal information used to open a bank account. As retailers begin to use Open Banking for identity verification (as well as payments) cybercriminals will swoop in to take advantage. According to the OBIE (Open Banking Implementation Entity) API calls have increased from 66.8 million in 2018 to almost 5.8 billion in 2020. A must in the payments ecosystem is robust API security measures.[xx]

Digital identity is a key enabler in data theft and ultimately financial fraud. Payment service providers and merchants must continue to put hardened structures in place to reduce the risk around the various types of identity fraud. But these structures must not prevent usability. FDP investments should focus on reducing synthetic identity and other misuse of identity accounts, including hijacking. The use of event-driven authentication, risk-based and behavioural biometrics, and AML checks is another area to explore to prevent exploitation of existing relationships.

### Figure 1.3: FTC Reported Identity Theft Cases 2020



*Source: FTC Consumer Sentinel Data Book 2020*

### ii. Cybercriminal Targeting Shifts

Analysis from Verizon's 2020 Data DBIR shows that 95% of all cyberattacks are financially motivated, with 70% of breaches being external actor initiated. However, the word external belies that fact that the majority of attacks are social in basis, with phishing being the tool of choice by cybercriminals the world over. Structures such as tokenisation of financial data are crucial, but they do not solve the issue of payment fraud alone.

Payment fraud is a lifecycle exercise and its mitigation must follow this lifecycle. A continued move by cybercriminals to reflect the omnichannel nature of the modern payment ecosystem is noted. Attacks are multifaceted; using manipulation of human behaviour to circumvent technological security solutions. In many instances, social engineering will be attempted via one channel of communication which will then contribute indirectly to an attack on another channel.

This approach provides fraudsters with a significant advantage, as many eCommerce merchants are focused on preventing fraud only at the transaction stage. Those without solutions to integrate against fraudulent activity on several channels will be left more vulnerable to fraud.

The COVID-19 pandemic has also created its own fraud focus, with channels that were driven into increased use seeing increased attention by fraudsters.

'The digital world is an anonymous environment, which was never designed with security in mind. This is compounded by the fact that fraudsters are highly creative – intentionally trying to defeat systems. Over the past year, there was a significant fraud focus on COVID-19 stimulus funds, which caused a dip in traditional fraud attacks like account takeover and online payment fraud. We believe we will see a rise in these traditional areas of fraud this coming year, as stimulus funding programmes dry up. […] We continue to observe phishing scams as a significant problem. In the coming year, account takeover, Card Not Present and account originations fraud schemes, including such variants as synthetic fraud and a surge in the use of stolen data used to create accounts, will resurface with fraudsters. We also believe that fraud schemes related to P2P (Person-to-person) payments and non-banking payment fraud are likely to be an issue in the near future.' – David Britton, VP Industry Solutions, Fraud & ID Management at Experian.[1]

### iii. Key Takeaways

The use of omnichannel and multi-faceted attack chains make any response to payment fraud more complex. This situation reflects the ecosystem model that has opened up payments and provided much-needed innovation for online transactions. The response must itself use an ecosystem of security methodologies that can be applied in a flexible manner depending on risk-level. This includes:

- Zero Trust Payments: The use of social engineering as part of the complex web of payment cybercrime looks like it will continue. If the work from home movement persists after COVID-19, this use of human manipulation and trickery is likely to continue unless structures are put in place to prevent phishing and reduce security hygiene gaps. However, if the basics of identification – meaning, identity verification and robust authentication – are in place, the process of payment fraud can be impacted and attacks reduced. Even if a credential is stolen and account takeover happens, if verification occurs as expected using a Zero Trust approach any payment fraud attempts could be stopped as they happen. How to achieve this requires a highly flexible approach to taking payments and would have to work across all channels. By placing the emphasis on data rather than identity, the prevention of fraudulent payments could be achieved. The concept of identity needs to evolve to include a 'longitudinal view' of a consumer's activities and payment behaviour, such that anomalies to that profile would immediately signal potential suspicious behaviour. Identity is not about the static, traditional identifiers, but is also about the behaviours normally associated with the identity.

  Persistent identifiers have the problem of being a sitting duck for cybercriminals to target. Zero Trust can and should be applied to payments; 'never trust, always verify' would remove the negative elements of a persistent identifier by always checking an element of an individual's claim during a transaction. This approach could reduce the reliance on onerous KYC processes by also making KYC a fluid entity, feeding data back into the KYC system as individual's make payments, building profiles that are harder to create synthetic versions of. The payments industry is moving slowly towards a more ZTA (Zero Trust Architecture) and the latest NIST (National Institute of Standards and Technology) advisory on a ZTA states that 'ZTA reduces risk and prevents any compromised accounts or assets from moving laterally throughout the network […] goal to prevent unauthorised access to data and services coupled with making the access control enforcement as granular as possible.'

  As payment networks become increasingly complex and cover multiple channels, this more fluid way of checking an event may well be the best way forward in payment security.

- Identity networks are likely to be increasingly used to provide verification events, as well as orchestrating data. This is likely to include the use of Open Banking to provide payments as well as identity

[1] Juniper Research interviewed David Britton, VP Industry Solutions, Fraud & ID Management at Experian in March 2021

assurance. These networks are based on API exchanges and focus must be placed on API security.

- Security awareness training should be provided to all technical and IT personnel to ensure that they understand the importance of security. This should include the use of security training and certification for key personnel to ensure an understanding of security configurations to avoid misconfiguration.
- Verification both during registration and during a transaction should use multiple sources of data if at all possible. This improves probability that single or dual sources are compromised. Verification to a high level of confidence will require a specialist third-party identity and orchestration services.
- Robust authentication, including transaction authentication and behavioural biometrics is an option that is likely to increase in availability in the next five years. Juniper Research estimates that by 2024, biometrics will be present on around 90% of smartphones. This factor will influence the choice of authentication in this channel. Also, certain transaction checks could initiate a step-up of authentication, depending on risk level.

## 1.4 Future Challenges and Open APIs

### 1.4.1 Open Banking APIs

A new report entitled 'Open Banking: revolution or evolution?' found that 87% of countries have some form of Open Banking APIs in place.[xxi] This initiative originated in the EU's PSD2 (Payment Services Directive 2) regulation and after a slow start, the novel idea of allowing individual and business banking data to be used for third-party service has taken off.

Open Banking data access is provided by thousands of banks across the world. The UK's Open Banking initiative, OBIE has over 100 Open Banking-enabled apps available in its Open Banking App store.[xxii] The framework of Open Banking is based on trust: A standardised framework based on trusted digital certificates are used to automate identification of stakeholders in an Open Banking-enabled ecosystem. In the UK, OBIE is about to transition to a new open finance service that will handle the centralised Open Banking directory, maintain technical standards, and enable future improvements. Together with the OpenID Foundation, OBIE has worked to define the FAPI (Financial-grade API) security profile, a secured standard for the sharing of sensitive payment data. Anti-fraud capability is high-up on the agenda of OBIE and its new service framework.

### 1.4.2 The API in the Machine

Open Banking continues to make strong roads into the payments system and is seeing traction in identity verification and assurance too. Companies such as Mastercard are embracing the capabilities with their Open Banking Connect platform; enabling its 2.6 million credit card customers to pay their balance using electronic payment services. A recent partner to this service is Lloyds Bank Group; allowing customers to pay using Mastercard Open Banking via an app to make payments, transfer money, and make withdrawals. A report from Temenos and the EIU (Economist Intelligence Unit) found that 87% of countries have an Open Banking initiative. As such, industry should expect Open Banking to become an intrinsic and deeply integrated part of the payments ecosystem.[xxiii]

Having open access to bank data, under user control and consent, is regarded by many countries as highly innovative in an era of hyper-connected ecosystems built on data. The API Playbook has been developed in Singapore by the Association of Banks and MAS (Monetary Authority of Singapore).[xxxii] This initiative is helping keep Singapore at the forefront of digital banking by offering API interfaces to build innovative customer experiences. The API Playbook also operates in the PSD2 area by offering support for seamless KYC; a vital part of the identification process that, when done well, can improve security.

The 'Open Banking Tracker' portal keeps watch on the progress of financial institutions in implementing Open Banking and use cases that are enabled using Open Banking APIS. One such example is PayPal's use of Tink's TPP (Third Party Providers) Open Banking and account aggregation service. PayPal has subsequently made a strategic investment in Tink.[xxiv]

API testing is a crucial aspect of ensuring security is robust. A rush to integrate with Open Banking APIs and other ecosystem APIs should not compromise the testing of the solution end-to-end and for the whole user journey, including alternative pathways and channels.

The EBA (European Banking Authority) Final Report on Guidelines on ICT (Information and Communication Technologies) and security risk management recommends the principle of the weakest link as 'third-party service providers, vendors and vendors' products may become channels to propagate cyberattacks. As payment ecosystem players are often integrated via open API connections, this weakest link principle needs to encompass API security best practices. API testing is essential to ensure API connections are hardened across the payments ecosystem: Tests should include vulnerability hunting across the entire API attack surface and tools should include black box fuzzing, SAST (Static Application Security Testing) – during development – and DAST (Dynamic Application Security Testing).

Juniper Research recommends having robust vendor management that extends to API security; this is a must when utilising any API for added functionality in an extended ecosystem.

## 1.5 Consumer Behaviour and Bots, a Wealth of Opportunities for Fraudsters

Consumers continue to be a complex area of security for payment providers. A mix of fear, ambiguity, and lack of security awareness creates a difficult user journey for merchants, banks, and ecosystem players alike. The COVID-19 pandemic has placed a new layer onto this environment. Prevented from going to brick-and-mortar shops, consumers have been going online. A report from payment fintech Rapyd found that nearly 60% of China-based consumers bought online more than normal, and in the United States, over 40% of consumers said they were making more online purchases. Also, over half of respondents said they bought goods online that were outside of their country of residence.[xxv]

Bots are adding to the behaviour issues inherent in securing payment systems. The report 'The big bad bot problem 2020' found that 62.7% of bad bots on a login page can mimic human behaviour and 57.5% of bad bots on the checkout page can simulate human behaviour when performing carding attacks.[xxvi]

As we have seen in part one, scams increased during COVID-19 and took advantage of the work from home movement and increasing merger of personal devices/credentials for corporate use and vice versa. Efforts by the cybercriminal community to create 'as-a-service' cybercrime tools that begin with human intervention has made the fraud industry highly accessible.

The connected payment universe, created by the advantages offered by an API economy and augmented by pandemic-related shifts in working patterns and home life, has opened up new points of entry and execution that allow cyber-attacks to propagate.

The continuing mosaic implementation of SCA (Strong Customer Authentication) requirements and late delivery of the regulation, coupled with a resistance from consumers to accept more stringent authentication, opens opportunities for cybercriminals to take advantage of social engineering. The increase in the UK to £100 for contactless payments that may be replicated across the EU may also prove to be a red rag to a fraudster.

### i. Type of API attacks

Security issues with Open Banking APIs fall into one of four categories:

- Unauthorised API requests
- Unauthorised modification of requests or token responses
- Unauthorised token use
- Exposure and modification of API response data

#### *a) Unauthorised API requests*

To prevent API requests from unauthorised parties, all requests should be digitally signed with a strong algorithm and the signature must be verified against a public key available on a public JWKS (JSON Web Key Set) endpoint. In addition, or alternatively, mutual TLS (Transport Layer Security) should be established between the Provider and the requesting party.

#### *b) Unauthorised modification of requests or token responses*

Because authorisation codes and multiple tokens may be returned as part of the OIDC (OpenID Connect) flow, it is vital that these cannot be substituted in man-in-the-middle-type attacks. For this reason, hashes of access tokens and authorisation codes must be included in the ID token and verified to ensure that all responses belong to the same request. In addition, Pushed Authorization Requests should be considered, or the use of form posts with signed JWTs (JSON web tokens) to avoid sending potentially sensitive codes as query string parameters.

#### *c) Unauthorised token use*

Most access and refresh tokens are of the bearer type, meaning that whoever has them can use them. From this, there are clear security implications. Often this vulnerability is mitigated by short token lifetimes, but this approach has limited value; better is to require digital signatures by the RP on token use and or use or mutual TLS.

*d) Exposure and Modification of API response data*

It is crucial that any response data (from use of access tokens) is properly protected, both through use of encryption and digital signatures.

### ii. API Authentication Security

Despite a delay in the ratification of the RTS (Regulatory Technical Standards) by the EU, the prevailing view has been that the directive’s demand for ‘secure’ access to banking services will be facilitated by the use of APIs to control and verify both users and information access. In a boost for secure access, screen scraping will not be allowed under the final draft of the RTS; avoiding a potential channel for fraud. Therefore, via APIs, banks will be able to more effectively monitor and control account access.

PSD2 and discussion about technical standards has not fallen on deaf ears in markets outside the EU. Indeed, in a desire to maintain a competitive edge across North America and parts of Asia, several organisations are focused on opening up their services via Open Banking APIs. Therefore, the potential for a wide number of players to offer financial services across the globe will only increase.

The emergence of an API that links third-party service providers to end users’ financial accounts undoubtedly opens up a new attack surface for cybercriminals. The threat here is twofold:

- How can FIs (Financial Institutions) ensure that API calls are made by trusted parties?
- How can API developers ensure that the business logic rules behind the API are not abused?

In the first instance, it is important to ensure that even if a user has a session open with, for example, a banking web app, the session ID cannot be used as an authentication mechanism for any API call. Indeed, this would leave the bank vulnerable to a Cross Site Request Forgery attack.

The use of a token-based approach to authorisation, with OIDC (OpenID Connect) as the underlying protocol, will prevent such attacks, assuming the protocol is used appropriately, with attention to use of the state and nonce options together with proper handling of signatures and refresh tokens.

These JSON web tokens, issued during the OIDC protocol, carry the information as to what resources can be accessed and are digitally signed to prevent tampering; other steps should also be taken so that only the authorised user of the token can make use of them. Use of these access tokens means that the system can be stateless and sessionless; relying on the token to determine authentication and authorisation for each API request. Security can be enhanced by applying a short lifetime to these tokens or limiting them to a single use.

One danger posed by OAuth2 (Open Authentication 2) or OIDC protocols are refresh tokens; these long-lifetime tokens may be issued to enable new access tokens to be requested without requiring re-authentication. However, because of their long lifetime, it is critical that they are stored securely by the token recipient.

The OBIE is attempting to standardise Open Banking in the UK, based on an enhanced version of OIDC. The result is an alignment between the OIDF (OpenID Foundation) and the FAPI Working Group. This will focus on developing improved security for the stakeholders' ecosystem, including customers.

This focus on collaboration to ensure security is part of the design remit of best-in-class solutions and should be one that permeates the entire industry as cybercrime presents increasingly sophisticated challenges.

### iii. Avoiding Logic Abuse

Ensuring that only trusted entities have access to APIs is only a part of API security. This is particularly pertinent here, as identity and account fraud grows in prevalence and as mechanisms for cybercriminals to steal money proliferate.

Controls must therefore establish that the originator of the API call is not overstepping their boundaries. API maintainers must be mindful of the fact that it is very likely, in many instances, that API calls will be made by 'trusted parties' with relatively little experience in managing the challenges of cybersecurity. They should be treated as compromised entities in terms of how they are monitored and allowed access to internal services with possible actions controlled by an underlying policy engine. The key points to consider are:

- Implementation of proper API restrictions.
- Protection against XML (Extensible Markup Language) and JSON digital signature attacks.
- Ensuring that communications are properly encrypted and signed.
- Limiting the number of possible API calls per day.
- Monitoring contextual data, such as time of day, to help detect possible fraudulent requests.
- Properly logging calls and metadata, and integrating this with the cybersecurity and fraud team.

It must be noted that these methods of securing APIs, including OBIE, only address the more obvious issues of using APIs for finance. In practice, social engineering attacks, malware infections of trusted parties, and sophisticated man-in-the-middle attacks cannot be addressed by protocol security alone.

Furthermore, there are a number of financial aggregation sites; offering a single-point API access (proxy service) to a number of FIs; the APIs exposed by such services may not be as secure as those implemented by the supported banks, but still allow payments and account management facilities, and so expand the attack space considerably. A set of security standards for banking/identity APIs is needed. Applying AI (Artificial Intelligence) to API security enforcement can offer a way to define more flexible rules that can reflect changing conditions.

APIs in the finance sector are proliferating which can cause issues with visibility and management. Lack of visibility opens up opportunities for stealth malware to operate. A number of solutions are coming onto the market that use AI to analyse API behaviour and spot patterns and anomalies that predict a cyberattack. However, as a caveat, algorithms may assume that API usage is consistent; this could potentially reduce the effectiveness of the security offering. However, it is worth exploring AI-driven API security in the future.

## 1.6 Real-time Payments

Although real-time payment infrastructure has been in place in some areas (such as the UK’s Faster Payments System), 2017 was a key year when such capability was extended to major digital commerce markets. Notably, both the US and SEPA (Single Euro Payments Area) zone launched such capabilities in November 2017, while Australian banks launched their own services in February 2018. A number of other launches have taken place during, or were planned for, 2018, with further roll-outs planned in the future.

Meanwhile, a full list of global instant payment schemes is presented in tables 2.2. The US is joining the instant payments area. The Federal Reserve was due to launch the FedNow service in 2021 but the COVID-19 pandemic has put this back until 2023. The service is designed to facilitate end-to-end faster payment services to financial customers. So far, 110 participants have signed up to help with testing to ensure market-readiness. Rules drive the FedNow scheme, including processing credit transfers of $25,000 or less in real-time on a 24x7x365 basis and meeting the ISO (International Organization for Standardization) 20022 standard. Rules on verification, such as customer validity during a payment, augment the service’s security. The limits of amounts may change during the consultation and pilot stages.

‘Real-time payments are already on the rise and will continue into the future across bank-to-bank, card-to-retailer, and even person-to-person payments. This requires automated tools as the market is moving to low latency, high volume activity, particularly fuelled by the ongoing growth in the digital marketplace. The faster the decisions are made, the better the user experience, but also the greater the challenge to get the fraud and trust decisions right.’ – David Britton, VP Industry Solutions for Fraud & Identity Management, Experian.

**Figure 1.4: Global Instant Payments Market Status**

| Country | Scheme Platform | Instant Payments Launch Year |
|---|---|---|
| Japan | Zengin | 1973 |
| Switzerland | SIC | 1987 |
| Taiwan | CIFS | 1995 |
| Iceland | RTGS | 2001 |
| South Korea | KFTC | 2001 |
| UAE | UAEFTS | 2001 |
| Brazil | SITRAF | 2002 |
| Mexico | SPEI | 2004 |
| South Africa | RTC | 2006 |
| Kenya | M-Pesa, PesaLink | 2007 |
| Chile | TEF | 2008 |
| UK | FPS, Paym, Pingit | 2008 |
| China | IBPS | 2010 |
| India | IMPS | 2010 |
| Nigeria | NIP | 2011 |
| Poland | Elixir Express | 2012 |
| Sweden | BIR, Swish | 2012 |
| Turkey | RPS | 2012 |
| Sri Lanka | CEFTS | 2013 |
| Colombia | CENIT | 2014 |
| Denmark | NETS RT, Mobile Pay | 2014 |
| Singapore | FAST | 2014 |

*Source: Juniper Research*

Awareness of instant payments by industry is at a high, with a PYMNTS report showing that 85% of organisations have instant payments on their roadmap for implementation in the next three years.[xxvii] Effectively, real-time payment infrastructure enables any payment instrument – such as credit transfers, direct debits and card payments – to be processed within seconds; avoiding the days-long process that was previously in place. This has substantial implications, particularly for SMBs (Small and Medium Businesses). Service and product supply contracts between businesses often involve a lag time between an invoice being issued and payment arriving in the beneficiary's account. The end effect is one of financial pressure, where SMEs are forced to seek credit to address shortfalls before incoming payments are received. Instant payments will reduce the burden from high interest rate, short-term loans; allowing SMBs to devote more funds on product development and quality, thereby improving competitiveness.

AI and machine learning come into their own when tackling instant payment fraud. The sheer volume of transactions and the need for faster payments means that any rules-based systems are simply not able to handle speeds where a transaction must be completed in a few seconds. Only AI-enabled fraud checks can handle massive volumes, coupled with fast speed of transaction. However, these smart systems should always be used along with knowledge of the techniques used by fraudsters. AI-enabled anti-fraud detection for instant payment fraud is part of the toolkit of the expert analyst, not a replacement for the analyst.

'Real-time and instant payments are here now and will continue to grow into the future. The fact that it is real-time is not a concern for Experian, as our solutions are designed to operate in low latency environments with high availability. However, it is important to be able to make the right decision in those very tight operational windows and to do so by leveraging a comprehensive set of data. This is where the use of machine learning excels, as it can be applied to a rich set of data features in every decision, in order to derive more accurate outcomes.' – David Britton, VP Industry Solutions, Fraud & ID Management at Experian.[2]

### 1.6.1 Fraud & Payments

Payment options are themselves creating dichotomies because of fraud prevention. Whilst in PSD2, card present rules have been derogated to allow a more seamless UX (User Experience); instead, they have a rule to prevent cards being used six times in a row. This consecutive exemption rule is commonly used across other regulatory jurisdictions and COVID-19 has had its own impact of this and the limit rule. In the UK, as mentioned, the FCA (Financial Conduct Authority) is looking at increasing the limit, at least temporarily from £45 to £100 ($63-$140). Any related increase in cumulative value is yet to be determined. In the EU, Mastercard raised its limits to 50€, and a request to raise the cumulative limit for contactless transactions to 250€ has been made by Digital Europe.

In other geographies, Australia has temporarily doubled its contactless limit from AUD100 to AUD200, whilst Singapore has increased its contactless limit from SGD100 to SGD200.

Having a transparent UX is an important lesson in the balance of fraud prevention vs usability. The impact of COVID-19 on decisions around the balancing act of user needs and anti-fraud measures, will, however, open

[2] Juniper Research interviewed David Britton, VP Industry Solutions, Fraud & ID Management at Experian in March 2021

up avenues of fraud. This fine balance is always the pivot upon which cybercrime turns.

Real-time payments require real-time fraud detection instruments. APP (Authorised Push Payment) scams, e.g. where fraudsters trick a consumer into paying large sums of money into a fraudster's bank account, are prevalent and have many ways to perform a scam all centred around either a malicious payee or a malicious redirect. According to UK Finance, during the first half of 2020, there were 66,247 cases of APP fraud totalling losses of £207.8 million. The UK Finance review 'Fraud 2020: The Facts' found that use of advanced security systems by FIs prevented more than £1.8 billion of unauthorised fraud. However, criminals stole over £1.2 billion through fraud and scams in 2019. The fight continues but with good news for FDP vendors.[xxviii]

### i. Problems Inherent in Infrastructure & Processes

In some countries the roll-out of instant payment schemes has been at odds with the infrastructure used by the banks. For example, the Vipps scheme, which is highly popular in Norway, enables instant P2P (Peer-to-Peer) mobile transactions, with money received via the app free to be spent immediately.

These same issues, i.e. the inability to respond to the demands of new payment schemes, will likely impact the rapid take-up of cross-border schemes, such as SEPA Instant Credit and the Eurosystem scheme, TIPS (TARGET Instant Payment Settlement), that allow individuals and firms to transfer money within seconds. By the end of 2021, PSPs (Payment Service Providers) adhering to the SCT Inst scheme and are reachable in TARGET2 will also be 'reachable in TIPS via a central bank money liquidity account, either as participants or as reachable parties.'

Instant payment schemes do not offer the same consumer protections against fraud (i.e. chargebacks) and Juniper Research still expects cards to be the favoured payment instruments in the medium-term, due to their greater consumer protections. This is even more likely to be the case if the payment limits on cards stays at an inflated level. There is opportunity for third-party vendors to offer similar consumer protections to help drive instant payments' uptake.

The European Payments Council's 'Payment Threats and Fraud Report 2020' retains its position from the 2019 report on the human-aspect of fraud; stating that the 'targets are users rather than technology.' Deception scams and impersonation are key methods behind direct debit fraud and SEPA Credit Transfer scams.

The report identifies a shift from consumers, retailers, and SMEs to company executives, employees (through 'CEO fraud'), PSPs and payment infrastructures – and a move to authorised push payments (APP) fraud.[xxix]

Whilst social engineering is a major threat, malware – including ransomware – should not be forgotten, as this appears to be increasing. The report continues; pointing out that APTs must also be dealt with as the use of advanced persistent threats are 'most sophisticated and lucrative types of payment fraud.'

The use of multiple channels of attack underpinned by human elements, such as impersonation, deception, phishing, account takeover, and 'old-school' lost and stolen card fraud, means that fraud detection cannot be a one-size fits all. Instead, smart detection tools can act as a barrier to fraud, rather than a hard stop; a piece of a bigger jigsaw puzzle where technology and analyst work together.

< >

# 2. Online Payment Fraud: Competitor Analysis

## 2.1 Introduction

Given the breadth of vendors involved in the FDP landscape, this section will look at a select number from across the ecosystem, so should not be seen as an exhaustive list. It also compares these players as far as possible; using criteria such as company size, breadth of service offering and funding. Those assessed here are shown below, with parent companies indicated in brackets, if applicable.

- Accertify
- ACI Worldwide
- Cybersource
- Experian
- Featurespace
- FICO
- Fiserv
- GBG
- TransUnion
- Kount, an Equifax Company
- LexisNexis Risk Solutions
- Microsoft
- NICE Actimize
- NuData
- SAS
- Riskified
- RSA Security

## 2.2 Juniper Research Leaderboard

Our approach is to use a standard template to summarise vendor capability. This template concludes with our views of the key strengths and strategic development opportunities for each FDP vendor.

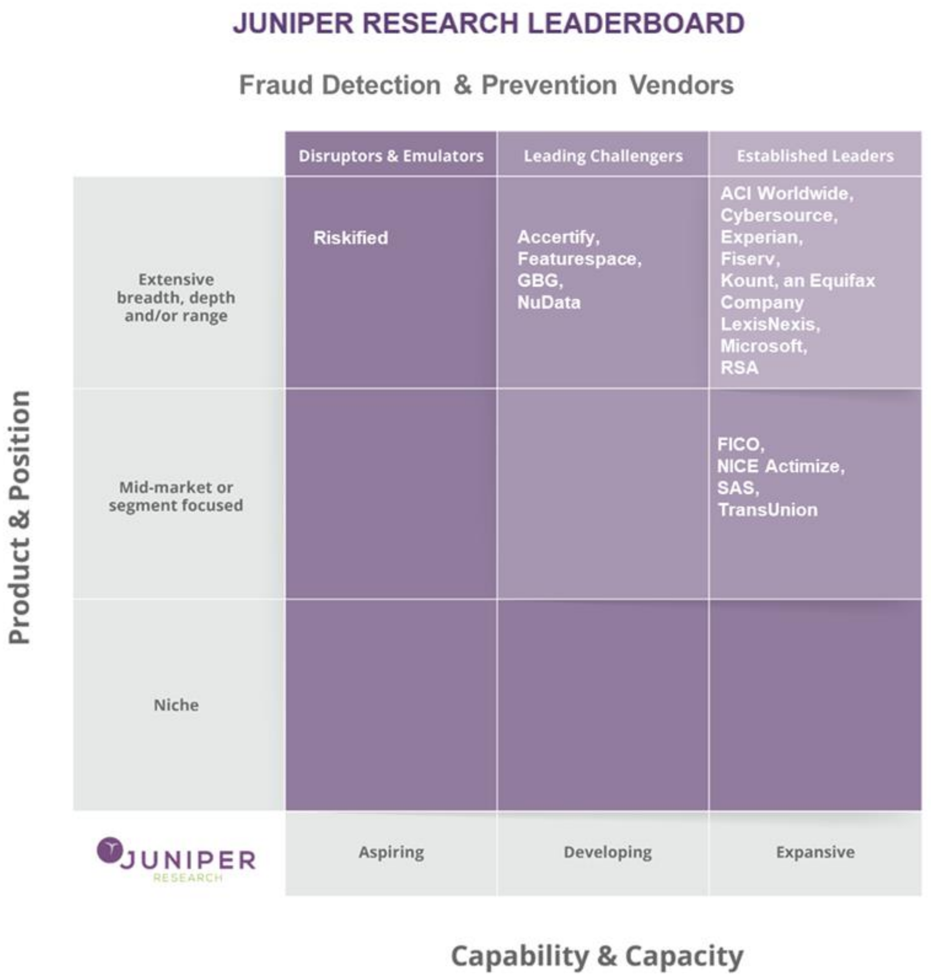
This technique, which applies quantitative scoring to qualitative information, enables us to assess each vendor’s capability and capacity and its product and position in these markets. The resulting Leaderboard shows our view of relative vendor positioning.

### Table 2.1: FDP Vendor Capability Assessment Criteria

| Category | Criteria | Description |
|---|---|---|
| Capability & Capacity | Financial Performance in Sector | In assessing this factor, we considered the vendor's FDP performance as measured by revenue, number of employees and investments. |
| | Experience in Sector | Experience of the vendor, as measured by the length of time FDP solutions have been offered. Acquisitions and experience are taken into account here. |
| | Operations & Global Reach | This factor considers primarily the overall extent of the vendor's geographical penetration, based on numbers of countries, regions, customers and offices to measure global reach. |
| | Marketing & Branding Strength | The strength of the vendor's brand and marketing capability as perceived by a review of the company's website; aspects such as use of case studies, communications and 'joined-up' marketing of total solution packages were considered. The extent to which vendors have marketing or distribution channel partnerships in place, e.g. in-country sales specialists and VARs (Value-added Retailers). |
| | R&D Spend | An indicator of the investment a vendor is making to develop best-in-class solutions; M&As (Merger and Acquisitions) are considered here as a measure of investment. |
| Product & Positioning | FDP Product Range & Features | This factor relates to breadth of product range coverage by platform, technology and channels. |
| | Customers & Deployments | We evaluate here the vendor's success to date, measured by the number of customers to whom the vendor has sold its FDP platform. This criterion is designed to balance the global reach criterion, by evaluating the experience of vendors that are well established in a single country, but not elsewhere. |
| | Partnerships | The extent to which a vendor has been able to achieve partnerships in the segment, with a view to augmenting its FDP capabilities. |
| | Creativity & Innovation | This factor assesses the vendor's perceived innovation through its flow of new features, products, developments and improvements. |
| | Future Business Prospects | This factor relates to the business' ability to develop and compete against others in the future. |

*Source: Juniper Research*

Figure 2.2: Juniper Research Leaderboard: FDP Vendors



JUNIPER RESEARCH LEADERBOARD

Fraud Detection & Prevention Vendors

| | Disruptors & Emulators | Leading Challengers | Established Leaders |
|---|---|---|---|
| Extensive breadth, depth and/or range | Riskified | Accertify,<br>Featurespace,<br>GBG,<br>NuData | ACI Worldwide,<br>Cybersource,<br>Experian,<br>Fiserv,<br>Kount, an Equifax Company<br>LexisNexis,<br>Microsoft,<br>RSA |
| Mid-market or segment focused | | | FICO,<br>NICE Actimize,<br>SAS,<br>TransUnion |
| Niche | | | |
| | Aspiring | Developing | Expansive |

*Source: Juniper Research*

Experian continues to invest into its FDP solution and uses the company's vast array of customer data to deliver an effective set of solutions across the entire consumer journey, from onboarding, through account management/account takeover and transaction risk mitigation. Experian leverages a combination of proprietary solutions and partner capabilities and data – integrated via its CrossCore platform – where it leverages a robust machine learning approach that takes into account these dynamic sources of data. The CrossCore platform's wide range of abilities, including the ability for clients to integrate solutions from third-party vendors via a single API, leveraging powerful orchestration and a hybrid machine learning approach to drive great accuracy in detection, with minimal false positives. This combination of capabilities makes it highly valuable across the online payment fraud environment.

### 2.2.1 Limitations & Interpretations

Our assessment is based on a combination of quantitative measures where they are available (such as revenue and numbers of employees) that will indicate relative strength, and also of qualitative judgement based on available market and vendor information as published. In addition, we have improved our in-house knowledge from meetings and interviews with a range of industry players. We have used publicly available information to arrive at a broad, indicative positioning of vendors in this market, on a 'best efforts' basis. However, we would also caution that our analysis is, almost by nature, based on incomplete information and so for some elements of this analysis we have had to be more judgemental than others. For example, with some vendors, less detailed financial information is typically available if they are not publicly listed companies.

We also remind readers that the list of vendors considered is not exhaustive across the entire market but, rather, selective. Juniper Research endeavours to provide accurate information; whilst every information or comment is believed to be correct at the time of publication, Juniper Research cannot accept any responsibility for its completeness or accuracy: the analysis is presented on a 'best efforts' basis.

The Leaderboard compares the positioning of vendors based on Juniper Research's scoring of each company against the criteria that Juniper Research defined. The board is designed to compare how the vendors position themselves in the market based on these criteria: relative placement in one particular unit of the board does not imply that any one vendor is necessarily better placed than others. For example, one vendor's objectives will be different from the next and the vendor may be very successfully fulfilling them without being placed in the top right box of the board, which is the traditional location for the leading players.

Therefore, for avoidance of doubt in interpreting the board, we are not suggesting that any single box implies in any way that a group of vendors is more advantageously positioned than another group, just differently positioned. The board is also valid at a point in time: April 2021. It does not indicate how we expect positioning to change in the future or, indeed, in which direction we believe that the vendors are moving. We caution against companies taking any decisions based on this analysis: it is merely intended as an analytical summary by Juniper Research as an independent third party.

## 2.3 Experian Company Profile

**Table 2.3: Juniper Research Leaderboard: FDP Vendors**

| | Corporate: Capability & Capacity | | | | | Product & Position | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Financial Performance in Sector | Experience in Sector | Operations & Global Reach | Marketing & Branding Strength | R&D Spend | FDP Service Range & Features | Customers & Deployments | Partnerships | Creativity & Innovation | Future Business Prospects |
| Experian | 🟩 | 🟩 | 🟩 | 🟢 | 🟡 | 🟢 | 🟡 | 🟩 | 🟩 | 🟩 |

HIGH 🟢 🟩 🟡 🟠 🔴 LOW

*Source: Juniper Research*

### 2.3.1 Experian

*Juniper Research interviewed David Britton, VP Industry Solutions, Fraud & ID Management at Experian, February 2021*

i. Corporate

Experian is a global information services company which provides data and analytical tools to client companies around the world. It is a publicly listed company and trades on the London Stock Exchange (EXPN). It had revenue of $5.18 billion for the fiscal year ending in March 2020.

Key executives include Brian Cassin (CEO); Kerry Williams (COO); Steve Wagner (Global Managing Director, Experian Decision Analytics).

Perhaps best known as one of the biggest credit reporting agencies, the company's main business divisions include Data, Decisioning (both B2B) and Consumer Services (B2C).

The company's fraud solutions have historically been reported under its Decision Analytics segment. Evidence from its latest annual report suggests that the company's FDP offering became an increasingly important part of its portfolio, with demand for fraud prevention noted as a driver for segment growth across business regions.

The company has a long tradition of providing identity proofing services and around 22%-28% of revenue of the Decision Analytics division is attributed to identity checking and verification.

**Figure 2.4: Experian Financial Snapshot ($m), FY 2018-2020**

| | FY 2018 | FY 2019 | FY2020 |
|---|---|---|---|
| Revenue | $4,662 | $4,861 | $5,179 |
| Net Income | $815 | $701 | $679 |

*Source: Experian*

In April 2014, Experian acquired 41st Parameter, a provider of device identification technology for web fraud detection, for $324 million, to strengthen its risk-based identity authentication capabilities. The acquisition was part of Experian's goal to provide the most complete set of fraud detection and identity authentication capabilities in the market.

### ii. Geographic Spread

Experian's headquarters are in Ireland. It has further offices in 45 countries across the globe in six continents.

### iii. Key Clients & Strategic Partnerships

- Experian has a wide range of partners, some of which are not publicly disclosed. The company works with partners for a variety of categories including, behavioural biometrics (Biocatch), traditional biometrics (Daon), document verification (Mitek, Acuant, Onfido), call centre risk assessments (TrustID), email verification (Emailage), Alternative Data (Ekata, Global Data Consortium), and Mobile Phone Verification (Boku/Danal).
- In 2020, Experian partnered with FinScore, (a pioneer in telco data credit scoring for the unbanked and underbanked populations in the Philippines). The partnership will help financial institutions reduce high default rates and prevent fraudulent activity, whilst simultaneously bridging the financial inclusion gap for unbanked individuals in the country.

### iv. High-level View of Products

Experian's ID and Fraud flagship solution CrossCore is designed to solve the major challenges that businesses face, specifically helping clients differentiate between their good and bad customers, without disrupting good customers or increasing customer friction in their attempts to stop fraud.

CrossCore combines an API with workflow, smart orchestration, and ML-driven decisioning functions. In doing so, it provides capabilities to pull in data from myriad sources to orchestrate decisions across the score and raw outputs of multiple risk and data services. Pre-designed templates allow deployment against various use cases, e.g. eCommerce use cases, identity driven on-boarding use cases, etc. CrossCore also has integrations with best-in-class vendors to add functionality where needed. This allows quick adaptation to the evolving fraud landscape.

In order to address these, the CrossCore platform provides:

- A single API with which clients can integrate for real-time assessments of ID verification, authentication and fraud risk for the user journey (account origination, login/account maintenance [non-monetary activities] and transactional activities).
- Sophisticated workflow orchestration: Where CrossCore can invoke calls to various services (Experian's solutions, backing capabilities or third-party vendors) based on conditional logic.

- Partner integration: Experian's partnerships extend beyond technical integration. It includes all contracting and due diligence with the vendor, so that the client only needs to amend their MSA (Master Service Agreement) with Experian to take advantage of the various partner solutions.

- Advanced Risk and Trust decisioning: CrossCore is designed to leverage the complete raw output in Experian's network to perform advanced analytics via Experian's native machine-learning infrastructure. Experian's approach includes a hybrid of unsupervised models (to generate features), supervised generic or custom models per use case, and a business rules infrastructure. This provides high levels of accuracy to the client; leading to significantly reduced friction and operational costs.

Behind CrossCore, Experian's native solutions include bureau-based ID verification, device intelligence (malware, jailbreak and device emulation detection), dark web intelligence, access to consortium risk attributes, machine learning-based risk modelling and case management/investigator tools.

'Experian Identity and Fraud business is a significant portion of Experian's overall portfolio of offerings, alongside our traditional credit bureau businesses, which operate in highly regulated markets. As we see more regulation being rolled out across various regions, particularly related to privacy, Experian's history makes us uniquely differentiated, and comfortable operating in heavily regulated environments. We serve clients across the globe, and for many of them, cross-border fraud is still a challenge. We are able to leverage that cross-border insight, so we can understand the behaviour patterns in our technology and adapt our risk strategies accordingly. Given that CrossCore is a global platform, we can also configure the solution to adapt to the requirements based on the jurisdiction, country, or client. For example, there may be heavier on-boarding and KYC in one region than another. Our solution allows each individual client to establish the specific protocols and select the appropriate services to be brought together to a single answer based on these requirements.' – David Britton, VP Industry Solutions, Fraud & ID Management at Experian

## Endnotes

[i] https://www.experian.com/decision-analytics/global-fraud-report

[ii] https://rusi.org/sites/default/files/the_silent_threat_web_version.pdf

[iii] https://www.cgi.com/uk/en-gb/blog/cyber-security/helping-defend-against-a-30000-increase-in-phishing-attacks-related-to-covid-19-scams

[iv] https://www.bbc.co.uk/news/technology-52319093

[v] https://info.abnormalsecurity.com/rs/231-IDP-139/images/AS_Qtrly_BEC_Report_Q3_2020.pdf

[vi] https://www.adobe.com/be_en/experience-cloud/digital-insights/digital-economy-index.html

[vii] https://newsroom.mastercard.com/asia-pacific/2020/05/20/contactless-payments-will-be-the-new-normal-for-shoppers-in-the-post-covid-19-world/

[viii] https://www.globenewswire.com/news-release/2020/11/19/2130156/0/en/86-of-global-consumers-fall-victim-to-identity-theft-and-fraud-as-online-shopping-increases.html

[ix] https://www.ecommercetimes.com/story/86591.html

[x] https://www.privacyaffairs.com/dark-web-price-index-2020/

[xi] https://www.riskbasedsecurity.com/2021/01/18/webinar-data-breach-trends-ransomware-jumps-by-100-and-records-exposed-hits-37-billion/

[xii] https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers

[xiii] https://www.cifas.org.uk/newsroom/survey-reveals-4-in-5-unprepared-for-2020-fraud-levels

[xiv] https://www.fenergo.com/assets/files/industry-knowledge/Reports/Another%20Fine%20Mess%20Report%20-%20APAC%20edition_FINAL_23.04.2020.pdf

[xv] https://www.thomsonreuters.com/en/press-releases/2017/october/thomson-reuters-2017-global-kyc-surveys-attest-to-even-greater-compliance-pain-points.html

[xvi] http://www.fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2020.pdf

[xvii] https://risk.lexisnexis.com/corporations-and-non-profits/credit-risk-assessment

[xviii] https://enterprise.verizon.com/en-gb/resources/reports/dbir/

[xix] https://www.helpnetsecurity.com/2020/04/14/home-work-cloud-security/

[xx] https://www.openbanking.org.uk/about-us/latest-news/three-years-since-psd2-marked-the-start-of-open-banking-the-uk-has-built-a-world-leading-ecosystem/

[xxi] https://www.temenos.com/wp-content/uploads/2021/02/Temenos-Open-banking-VFinal-1.pdf

[xxii] https://www.openbanking.org.uk/app-store/

[xxiii] https://www.businesswire.com/news/home/20210222005781/en/

[xxiv] https://tink.com/blog/open-banking/paypal-tink-extend-partnership/

[xxv] https://www.rapyd.net

[xxvi] https://blog.radware.com/wp-content/uploads/2020/03/Radware_Bot_Manager_The_Big_Bad_Bot_Problem_2020_Report.pdf

[xxvii] https://www.pymnts.com/news/faster-payments/2021/real-time-networks-getting-really-serious-about-fraud-in-2021/

[xxviii] https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2020

[xxix] https://www.europeanpaymentscouncil.eu/document-library/reports/2020-payment-threats-and-fraud-trends-report