ONLINE PAYMENT FRAUD

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

Deep Dive Strategy & Competition

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

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.

'eCommerce was growing up to 20% but we saw a huge inflection point in March last year, with a 50-60% increased online traffic. This plays into the hands of fraudsters. Before COVID-19, fraud was increasing at the same rate as eCommerce. Since the pandemic, this pattern is continuing – if a channel grows 20% the fraudsters also match this one-to-one. Why are we not making meaningful progress against fraud? This is a hyper dynamic environment, merchants and consumers are changing business and behaviour all the time and opening up new opportunities for fraud. It is, in fact, an achievement to keep pace.' – Andrew Naumann, Product Management, Cybersource (Visa).[1]

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.

'We are seeing a large increase in the way people are interacting with eCommerce in our own and our customers environments. The fraud shift is towards online. Fraudsters are capitalising on the fact there is a large number of commerce vendors who have not worried too much in the past about fraud, as online was a small percentage of their business (perhaps 10% or less). Suddenly, with COVID-19, there has been a push to eCommerce with businesses seeing over 90% of online sales, and fraudsters are following the money.' – Anand Oka, Partner Group Program Manager, Microsoft.[2]

[1] Juniper Research interviewed Andrew Naumann, Product Management, Cybersource (Visa) in March 2021.
[2] Juniper Research interviewed Anand Oka, Partner Group Program Manager, Microsoft in April 2021

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 complex web of interactions and the use of open APIs, 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 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.

'The modern shaped vernacular is around the customer experience and building trust using identity. A lot more CNP transactions are being seen during the pandemic, this means that more data and behavioural change is being generated to feed machine-learning models to reduce false positives. You can say that the pandemic has improved the accuracy of the models and the rise of the digital identity network has also helped shape this. The fraudsters, however, are also increasingly focusing on payments.' – Vikram Dhawan, Vice President and Senior Product Leader, Kount, an Equifax Company.[3]

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.

  'It is an essential for businesses to create trust in the digital world, for companies to trust users to onboard them and for users to trust the companies too. Digital transformation has accelerated by five to ten

[3] Juniper Research interviewed Vikram Dhawan, Vice President and Senior Product Leader, Kount, an Equifax Company in March 2021

years and fraud is also becoming more complex, so there is a need for solutions that meet both identity and fraud.' – Laura Barrowcliff, Head of Strategy, GBG PLC.[4]

- 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 is 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 address that matches the billing address, accurate AVS (Address Verification Service) data and card verification number, etc (ie 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 no anomalies to detect. The only option is to ask more questions, but this introduces friction to the buying process.

- 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 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.

[4] Juniper Research interviewed Laura Barrowcliff, Head of Strategy, GBG PLC in March 2021

- 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 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]

In this section, we examine the overall size of the eCommerce landscape. Meanwhile, industry fraud data will be analysed to frame the issue at hand.

Figure 1.1: Experian Fraud Statistics

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.

'[…] Had we been asked the question in 2020, what two types of fraud would we expect to see, I do not think anyone would have said benefit fraud or mule fraud. This is to do with unusual landscape changes. Ensuring that people who are responsible for fraud systems understand the triggers and restrictions is important in addition to the systems becoming more elastic and reactive to fraud events. AI is not a replacement technology but a supporting technology.' – David Sarjantson, Senior Director, Microsoft.[5]

1.2.1 Physical & Digital Goods

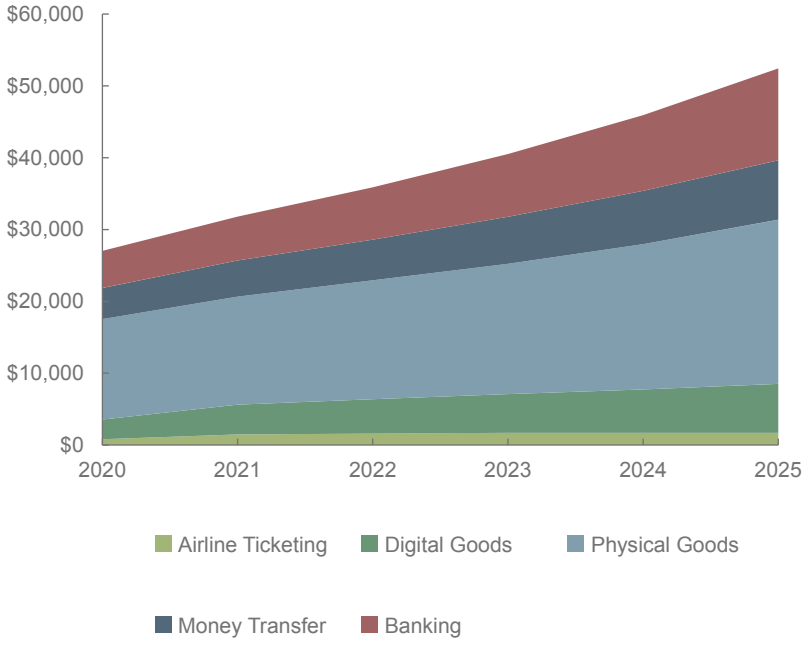
Juniper Research anticipates that by 2024, mobile is expected to account for 78% of physical goods fraud transaction value having risen from 63% in 2019. Growth in the mobile channel will be at a CAGR of 16.4% over the forecast period, compared with just 0.4% in the online space.

eCommerce has proven to be a lucrative hunting ground for fraudsters, especially as this was the only option open to buyers during lockdown periods caused by the COVID-19 pandemic.

As eCommerce continues unabated, the online payment of goods provides a feeding ground for fraudsters. Whilst fraudsters can dip into an immediately accessible range of victims, the sophistication of FDP (Fraud Detection & Prevention) solutions available to merchants and issuers means that fraud is, by and large, preventable, if one is prepared to invest. The enforcement of more robust identity checks and improvement in authentication requirements during transactions is also redressing the balance somewhat.

[5] Juniper Research interviewed David Sarjantson, Senior Director, Microsoft in April 2021

Figure 1.2: Total Value of Fraudulent Transactions ($m), Split by eCommerce Segment, 2020-2025



Source: Juniper Research

1.2.2 eCommerce Value

The total digital commerce market (including money transfer, remote goods purchases, digital banking, ticketing, digital gambling services and others) is expected to exceed $18 trillion in value by 2024, from $12 trillion in 2020.

Stay-at-home orders have meant that eCommerce spend has been dominated by remote physical goods purchases. This is expected to continue to some extent, as lockdowns continue to place pressure on high streets. Money transfers, either via dedicated platforms or banking services, will also account for a substantial proportion of the total spend. Digital banking, has also seen a surge because of pandemic pressures to perform banking tasks in a socially distanced manner without going to a local branch.

Meanwhile, merchants' accounts and card-on-file options have enabled one-click purchases for consumers, but this convenience has come at a price. Verification of identity has taken a back seat in favour of convenience which, in turn, has opened avenues for fraudulent activity. Indeed, as we shall see in the next section, identity theft is becoming a critical tool in the digital fraudster's armoury, suggesting that verification of the device being used, or its user, is no longer sufficient. More importantly, do the user or device's actions and behaviour match those of a genuine consumer? Being able to detect good behaviour is also an important role of detection and prevention solutions as this sets a baseline for detection of fraud.

As digitisation takes hold in the payment industry and omnichannel transactions become normal, the importance of robust KYC processes will become even more prominent. Moving those processes online will help balance user expectation, friction reduction and security.

Banks, in particular, are looking at online KYC in those terms, but also in terms of cost reduction, as offline KYC processes take time and can be costly. The use of an ecosystem approach that orchestrates data for relevant services, such as credit file agencies, AML engines and AI-based anti-fraud checks, can be used to achieve online KYC, reduce

friction, and improve the customer experience. Augmenting security with event-driven transactions, can also improve security. The general market view is that friction and security must be balanced against the level of fraud that a retailer is willing to accept.

'The trend is to be very sure that a customer is who they say they are, and from a fraud prevention perspective, it is critical to use data to validate a consumer's identity. We provide this element and balance it against the various data privacy constraints. […] How trust is built when building frictionless flows, is an ongoing question and one that will challenge the industry.' – Amanda Mickleburgh, ACI Worldwide[6]

1.2.3 Payments: Changing Dynamics & Expanding Ecosystems

Based on Juniper Research data, there are currently over 15 billion payment cards in issue. Whilst credit and debit cards continue to be the stalwarts of online payments, innovation in payments continues to encourage seamless and platform-integrated spending.

Initiatives, such as the BNPL model in the UK, offer easier credit, encouraging online sales. However, this model has come under heavy criticism during the pandemic. Fintechs such as Klarna have seen revenue increases of 31% but are also under threat of heavy regulation to prevent misuse by consumers who end up with large debts. The pandemic is also driving fintechs into new territory and Klarna, as an example, is working by tying up the loose ends of the payment ecosystem, the Klarna bank account being integrated with a Visa debit card and connected to both Google Pay and Apple Pay. The controls allow users to track and manage their everyday spending.

Mobile payment platforms have been the winners in a dreadful pandemic, as they offer a way to make COVID-19 secure payments. Mastercard saw a 40% increase in the use of contactless payments.[viii] A 2021 Global Insights report from Experian found that 60% of consumers are using a universal mobile wallet to make digital payments.

The payment ecosystem, driven by fintech innovations and mobile apps, and steered by a need to remain free of the coronavirus, has not only become more interwoven with our mobile devices, but is moving adults as well as children into the mainstream of online payments. Merchants too, are innovating, weaving new marketing strategies into the payment ecosystem, for example, smart speakers. The seamless experience between product, shop, and then payment, often via a mobile platform, focuses on improving the customer experience; these types of seamless experiences are perfect for social engineered fraud.

The COVID-19 pandemic, too has created new paradigms in the fraud ecosystem, as Rich Stuppy, Vice President and Senior Customer Experience Leader at Kount, an Equifax Company, told Juniper Research:

'In terms of COVID-19 relief fraud alone, 30 or 40 billion dollars of COVID relief have gone into fraudsters hands. In one state, over 100 million dollars fraud was committed from prisons. This money is then invested in the criminal trade to buy data, money mules, etc. This year will change the face of fraud for many years to come. […] The challenge continues as the ecosystem adjusts – in 2020, Kount even screened hundreds of

[6] Juniper Research interviewed Amanda Mickleburgh, Director Product – Merchant Fraud, ACI Worldwide in March 2021

transactions that came out of Antarctica.' – Rich Stuppy, Vice President and Senior Customer Experience Leader, Kount, an Equifax Company[7]

Globally, there is a mixed picture of payment type popularity. Payment via digital wallets is strengthening, especially in markets like China with WeChat. The big 'Pays,' (Apple Pay, Google Pay and Samsung Pay) continue to attempt to claw their way into the consumer retail space; in the US, adoption was slow but is now seeing an uptick, with vendor Blackhawk seeing 55% of US consumers surveyed saying they used a wallet to make a payment.[ix]

Digital assistants are only just beginning to be used for online banking and some integrated payments. A 2020 Juniper Research report has found that the total transaction value of smart home payments that occur via smart home devices, will exceed $164 billion in 2025, up from $22 billion in 2020.

The convenience and brand awareness forged by PayPal continues to dominate the ecosystem. New products such as the PayPal BNPL scheme, enabling payments to be spread over several months, allows the company to keep a firm grip on the payment ecosystem and compete with the likes of Klarna. PayPal also added a wallet facility for cryptocurrency in 2020. Investors have speculated this is a move to compete with Square's Cash App.

In 2020, the ECB along with 16 European banks launched the European Payments Initiative. This is a framework for a unified payment solution for consumers and merchants across Europe. The scheme provides for a payment card and a digital wallet for in-store, online, person-to-person payments and cash withdrawals. This unified card approach reflects other EU initiatives around data exchange and privacy. The reduction of a fragmented system with a unified replacement ecosystem is hoped will strengthen European providers.

One example of a European provider in this vein is Swish. Here is a breakdown of the company:

- Launched in 2012 by six local banks
- P2P money transfer using a mobile number
- 2020 saw 148% increase in use of QR codes
- 53% growth in use in Sweden

[7] Juniper Research interviewed Rich Stuppy, Vice President and Senior Customer Experience Leader, Kount, an Equifax Company in April 2021

Figure 1.3: Swish

Source: Swish

i. The Omnichannel Challenge

Customer expectations are now such that it is normal to present payment transactions for multiple types of channels. Experian, in its report '2020 Global Identity and Fraud Report' believed customer UX (User Experience) to be a pivot in the market:

'There is a need to provide a consistent 360-degree experience across the user experience and payment ecosystem. Onboarding of customers' needs to be seamless.'

'A trend in the use of ML is to enhance things that were standard, for example, fuzzy matching. This was built off older algorithm, but ML model are now being used within an identity sphere to provide better user experience.' — Laura Barrowcliff, Head of Strategy, and David Mirfield, Financial Crime and Risk, GBG PLC.[8]

1.3 Development of Fraudulent Activity

It is not surprising that as eCommerce transactions grow year-on-year, so do the number of fraudulent transactions. According to ACI Worldwide, which conducts an annual survey based on eCommerce growth and CNP (Card-not-Present) fraud. According to ACI researchers, the 2020 pandemic saw a 27% increase in non-fraud chargebacks in April, the airline industry taking the brunt as consumers looked to secure refunds for unused airline tickets. However, fraud remained buoyant during the pandemic with the average ticket amount increasing from $161 in 2019

[8] Juniper Research interviewed Laura Barrowcliff, Head of Strategy, and David Mirfield, Financial Crime and Risk, GBG PLC in April 2021

to $174 in 2020 per fraudulent ticket — this is double the average ticket price for genuine purchases in 2020.

Phishing incidents rose by 220% compared to the yearly average during the height of global pandemic. 52% of these can be attributed to failures at the access control layer according to F5.[x]

Fraud remains a top issue with 55% of businesses planning to increase fraud management budgets according to the 2021 Global Insights report from Experian.

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.

These findings are mirrored by ACI Worldwide who are seeing a tracking of fraud activity against increased online commerce driven by the COVID-19 pandemic. Research from ACI Worldwide found that the average fraudulent attempted purchase value increased by $36 in March 2020, which corresponds to a 13% increase in fraudulent attempted transactional value overall.[xi]

'Fraud is very holistic. Fraudsters think holistically. Just concentrating on payment fraud is not enough. Fraud often starts at the early stages, by creating fake accounts. Fraudsters are not naïve They attack in broad ways, such as creating fake accounts, en masse, for major events like Black Friday. Dynamics 365 has been designed to take this holistic approach to fraud into account. Look at a transaction, for example. It may look OK, not fraudulent at all. But then if you can tie it to a device that has been making multiple purchases across lots of retailers in a short time span, and perhaps that account is new, then this all starts to add up to a fraudulent transaction. It is this ability to make the transaction contextual, looking across the wider landscape that is powerful in fraud mitigation.' - Kapil Tandon, Core Product Lead, Microsoft.[9]

1.4 Key Trends in Digital Fraud

1.4.1 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 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.[xii]

Account takeover must be a focus, as account control can have long-reaching problems; a survey by TransUnion (iovation) of 1,068 adult

[9] Juniper Research interviewed Kapil Tandon, Core Product Lead, Microsoft in April 2021

Americans, found a 347% increase in account takeover and 391% rise in shipping fraud attempts globally.[xiii]

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. 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.

'In terms of eCommerce and consumer fraud, the challenges lie in how the technology layer solves this and how every transaction is verified across the entire ecosystem? This is complicated for the merchant and consumer, and they do not want to get in the weeds of how the integration works. ACI adds value in solving this problem. ACI is the glue that makes the ecosystem stick.' – Amanda Mickleburgh, ACI Worldwide.[10]

[10] Juniper Research interviewed Amanda Mickleburgh, Director Product – Merchant Fraud, ACI Worldwide in March 2021

1.4.2 Continued Darknet Activity & Messaging Apps

i. From Darknet to Clearnet

Dark web sites that sell on 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 found shows costs credit card data, payment processing services, and forged document. A PayPal transfer from 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.[xiv]

Figure 1.4: Average Pricing of Fraud Materials

Category	Product	Avg. dark web Price (USD)
Credit Card Data	Cloned Mastercard with PIN	$15
	Cloned American Express with PIN	$35
	Cloned VISA with PIN	$25
	Credit card details, account balance up to $1000	$12
	Credit card details, account balance up to $5000	$20
	Stolen online banking logins, minimum $100 on account	$35
	Stolen online banking logins, minimum $2000 on account	$65
	Walmart account with credit card attached	$10
Payment processing services	Stolen PayPal account details, minimum $100	$198.56
	PayPal transfer from stolen account, $1000 – $3000	$320.39
	PayPal transfers from stolen account, $3000+	$155.94
	Western Union transfer from stolen account, above $1000	$98.15
Forged documents	US driving license, average quality	$70
	US driving license, high quality	$550
	Auto insurance card	$70
	AAA emergency road service membership card	$70
	Wells Fargo bank statement	$25
	Wells Fargo bank statement with transactions	$80
	Rutgers State University student ID	$70
	US, Canada, or Europe passport	$1500
	Europe national ID card	$550

Source: PrivacyAffairs

Figure 1.5: Average Pricing of Fraud Materials, Continued

Product	Average dark web Price (USD)
Cloned Mastercard with PIN	$15
Cloned American Express with PIN	$35
Cloned VISA with PIN	$25
Credit card details, account balance up to $1000	$12
Credit card details, account balance up to $5000	$20
Stolen online banking logins, minimum $100 on account	$35
Stolen online banking logins, minimum $2000 on account	$65
Walmart account with credit card attached	$10

Source: PrivacyAffairs

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.[xv] 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 checks, no anti-fraud stone can be left unturned.

The result is that FDP 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.

Figure 1.6: Pricing for Fraudulent Materials

2020 Pricing (in USD): Bank Logs and Routing Numbers

US bank log - $100 USD balance	$25
US bank log - $4,000 USD balance	$55
US bank drop (account number, routing number, linked accounts)	$530
UK bank log - £3,000 GBP balance	$50
Germany bank log - €3,500 EUR balance	$300
Japan bank log - ¥400,000 JPY balance	$350

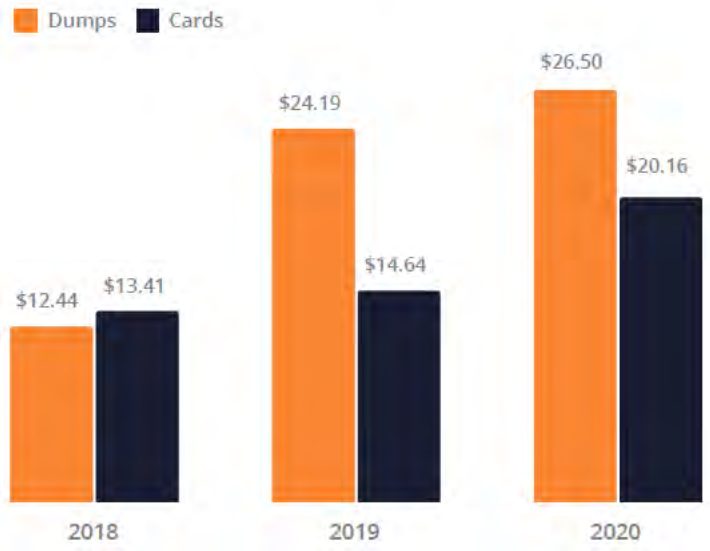
Source: Flashpoint

Figure 1.7: Pricing for Fraudulent Materials – Continued

2020 Pricing (USD): Exploit Kits for Phishing, Ransomware, and Others

Ransomware exploit kit	$9
Legacy ransomware, bundle of 9 types	$12
Tailored phishing page with tutorial	$35
Office365 exploit kit	$125

2020 Pricing (in USD): Payment Card Data



Source: Flashpoint

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.

1.4.3 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.[xvi] 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.

Figure 1.8: FTC Consumer Sentinel Network Snapshot 2019

Source: FTC

In the UK, CIFAS 90% warned of fraud spikes in 2020 and 2021 with the majority of people being unprepared.[xvii]

'There is a convergence between payments and identity. A parallel is with the information security industry over the last 20 years. In the late 90s, everything was siloed, protect PCs, protect servers, etc. Over time, all this became integrated, and everyone realised it was not just about protecting devices, it was about authorisation, access control and identity. This came together along with compliance. We are now seeing a 'growing up' of fraud, and fraud protection is becoming a first-class citizen in that world. Fraud prevention managers need to look end to end across the user journey. This is about all transactions, not just payments. Account creation attempts, account logins, returns, for example, could be

fraudulent. Throughout the lifecycle there are many attack types. You cannot just look at one type of fraud, as this limits your ability to detect fraud.' – David Sarjanston, Senior Director, Microsoft.[11]

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 types system, including potentially self-sovereign, may also offer verified claims that could be used to definitively identity 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. 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.[xviii] 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.[xix]

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.

'Looking at it from an innovation angle, faster payments transformed the customer experience, but created new fraud opportunities. The fact you could transfer large sums of money out of an account quickly, is attractive for the scammer. But regulations work both ways. PSD2 and SCA, for example, are a barrier to customer experience but a strong control to stop fraud.' – David Mirfield, Head of Product, Financial Crime and Risk, GBG PLC.[12]

Synthetic identity is where a cybercriminal uses snippets of legitimate data (like a Social Security Number) then add in other made-up data to

[11] Juniper Research interviewed David Sarjanston, Senior Director, Microsoft in April 2021
[12] Juniper Research interviewed David Mirfield, Head of Product, Financial Crime and Risk, GBG PLC in March 2021

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 found to be issued to a synthetic identity could be as high as 2.7% of all new accounts.[xx] 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.[xxi]

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.

'Fraud solutions need to be tightly integrated with authentication services, and post transaction too is an important realm to work in. The idea is to provide risk management services across all touchpoints in the transaction lifecycle – this includes lifecycles that cover click and collect as well as online.' – Andrew Naumann, Product Management Cybersource (Visa).[13]

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:

[13] Juniper Research interviewed Andrew Naumann, Product Management Cybersource (Visa) in March 2021

Figure 1.9: 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.
Paay (payment card processor)		Database containing 2.5 million card transaction records accessible online without a password.
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 the company's hacking software tools.

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.

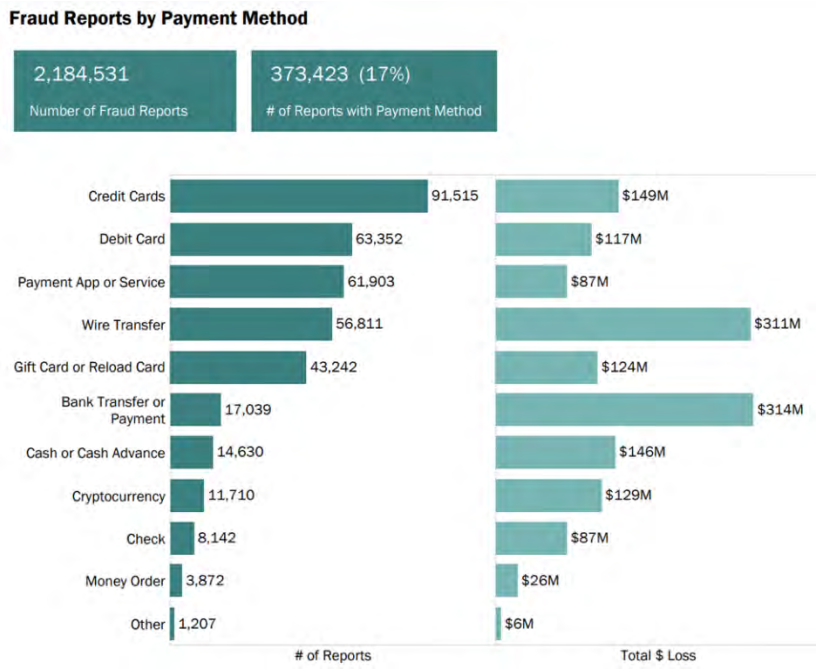
Whilst phishing is key in data breach events, misconfiguration and accidental exposure should not be overlooked. The 2020 Verizon DBIR (Data Breach Investigations Report) found 43% of all data breaches targeted web applications. During 2020, a noticeable increase in misconfigurations of web apps, servers,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

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.[xxiv]

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 1.10: FTC Reported Identity Theft Cases 2020



Source: FTC Consumer Sentinel Data Book 2020

Figure 1.11: Identity Theft Reports by Type

Theft Type	Theft Subtype	# of Reports	% Difference from Previous Year
Government Documents or Benefits Fraud	Driver's License Issued\Forged	6,161	+23%
	Government Benefits Applied For\Received	394,324	+2,920%
	Other Government Documents Issued\Forged	9,508	+42%
	Passport Issued\Forged	1,395	+85%
Credit Card Fraud	New Accounts	365,597	+48%
	Existing Accounts	33,852	+9%
Loan or Lease Fraud	Apartment or House Rented	13,524	+59%
	Auto Loan\Lease	72,535	+88%
	Business\Personal Loan	99,667	+127%
	Federal Student Loan	27,495	+88%
	Non-Federal Student Loan	17,125	+55%
	Real Estate Loan	11,845	+54%
Employment or Tax-Related Fraud	Employment or Wage-Related Fraud	26,645	+34%
	Tax Fraud	89,391	+225%
Phone or Utilities Fraud	Landline Telephone – Existing Accounts	2,090	+20%
	Landline Telephone – New Accounts	12,287	+13%
	Mobile Telephone – Existing Accounts	6,053	+8%
	Mobile Telephone – New Accounts	48,166	+9%
	Utilities – Existing Accounts	2,248	+55%
	Utilities – New Accounts	41,266	+39%
Bank Fraud	Debit Cards, Electronic Funds Transfer, or ACH	30,802	+32%
	Existing Accounts	13,704	+9%
	New Accounts	50,865	+87%
Other Identity Theft	Email or Social Media	14,086	+36%
	Evading the Law	4,705	-4%
	Insurance	8,600	+62%
	Medical Services	45,558	+64%
	Online Shopping or Payment Account	14,779	+38%
	Other	281,434	+69%
	Securities Accounts	3,779	+72%

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.[14]

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

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

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.

'Phishing is becoming the most onerous fraud point. Most fraudsters understand that most merchants have a robust fraud solution in place, so they go upstream to phish credentials to perform account takeover to take control of a user's reputation.' – Andrew Naumann, Product Management, Cybersource (Visa).[15]

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 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 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.

[15] Juniper Research interviewed Andrew Naumann, Product Management Cybersource (Visa) in March 2021

2. Online Payment Fraud: Market Dynamics

2.1 Introduction

In payments trends come and go, as technology advances are made. However, fraud is a persistent element of all digital approaches. Juniper Research has identified the following major trends that require focus in the future: Open Banking APIs, instant payments, regulations, consumer behaviour and social fraud, the fintech challenge and 3DS2 and biometrics.

We will analyse how these will impact the digital payments landscape in the context of fraud in the future.

2.2 Future Challenges and Open APIs

2.2.1 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.[xxv] This initiative originated in the EU's PSD2 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.[xxvi] 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.

2.2.2 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 use 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.[xxvii]

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 Open Banking and account aggregation service. PayPal has subsequently made a strategic investment in Tink.[xxviii]

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 Final Report on Guidelines on ICT 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.

2.2.3 FAPI

FAPI is a profile of OAuth used for high read-write risk access to highly sensitive data or write access to financial data. The FAPI specification sets out how the implementation of the protocol can be used to mitigate against attacks such as 'authorisation request tampering, authorisation response tampering including code injection, state injection, and token request phishing.' Version 2.0 of FAPI is currently in draft. FAPI is also part of the Open Banking specification and as Open Banking increases in uptake, FAPI implementation follows.

2.2.4 Open Banking, CIBA (Client-initiated Back Channel Authorisation) and Premium APIs

The Open Banking API specification standard must be used across the entire end-to-end token sharing process, including from the TPP (Third-party Provider, typically a service that connects to multiple banks using their Open Banking API) to the relying party. Some TPPs may not enforce the use of the Open Banking standard at the RP side of the flow. This should be checked when implementing an Open Banking-based payment service.

As Premium APIs are released by banks to recoup the costs of creating Open Banking APIs, these APIs must follow the Open Banking standards specification to ensure security.

CIBA allows for a decoupled flow and facilitates the secure process to Open Banking via other media, including in person and telephony, and can be used with smart devices (such as a TV).

The difference between CIBA and using decoupled authentication, for example, authenticating to the bank using a mobile device, is that with CIBA, the entire interaction with the provider bank is though the user's device, not just the authentication part. Therefore, it is more secure across the entire process; for example, it reduces phishing attacks. The browser is a weak point, CIBA avoids this.

An improvement to CIBA could be made by taking a leaf out of OAuth 2 Device Flow. Both use a code sent during transactions (known as a 'binding message' in CIBA). Device Flow connects this message during the transaction by ensuring the user enters the code during the transaction, thereby linking the end-to-end process up closely. CIBA does not do this and so opens a potential security gap.

2.2.5 PSD2 Overview

PSD2, which was adopted by the European Parliament in October 2015, came into force in January 2018. The EBA migration period was in due in December 2020. However, in the UK, the FCA has delayed this until end of June 2021. The introduction of PSD2 means radical changes for the financial industry. The directive enables so-called PISPs (Payment Initiation Service Providers; managing payments in and out of an account) and AISPs (Account Information Service Providers; allowed to retrieve account data) to emerge. Banks will be forced to offer these service providers a means of both accessing user account information, as well as enabling transactions to occur via one of the aforementioned intermediaries.

From a high-level perspective, PSD2's stated goals are to increase competition in the digital payments space, while simultaneously introducing new rules focused on more effective protections for the consumer. In the context of the latter goal, the EBA (European Banking Authority) has been working with the EC (European Commission) on developing a so-called RTS (Regulatory Technical Standards) framework for SCA (Strong Customer Authentication), along with common and secure communications.

'Whilst 3DS does provide merchants with a complaint solution for 2FA, it may also add friction to the consumer checkout experience and can result in lost sales. Therefore, it is strongly recommended that merchants maximise the exemptions available within the SCA regulation. Exemptions allow merchants to process in-scope remote payments without the need for 3DS. Exemptions can be requested on transactions up to the value of €500, subject to certain criteria, which can significantly mitigate the impact of SCA. In addition to the exemptions, merchants are not required to complete 2FA on transactions which are out of scope of the regulation, this means that payments made on cards that were issued outside of the EEA (European Economic Area) do not require 2FA. Identifying these out-of-scope payments can further mitigate the impact of SCA.' – Accertify.[16]

2.2.6 PSD2 State of the Nations

On 14th September 2019, the SCA component of PSD2 came into force. However, uptake is still continuing to be slow. A survey by Ravelin on the

[16] Juniper Research interviewed Accertify in March 2021

implementation of PSD2 shows the level of uptake of PSD2 and SCA across the world:

Fortunately, the EBA, with help from country-level regulators, such as the FCA, has extended the implementation schedule and has worked with UK Finance to create a plan of action. No enforcement actions would be taken against firms not complying with the SCA requirements from 14th September 2020, as long as evidence showing they are making efforts to do so can be supplied. The new date of full compliance is September 2021.

A Ravelin report into 3DS2 acceptance and delivery shows a generally good acceptance rate.

Figure 2.1: Ravelin 3DS2 Statistics

Source: Ravelin

Juniper Research expects that cybercriminals will take full advantage of any delays. There have already been phishing attempts based on the introduction of the SCA requirement.[xxviii] This delay will extend the period where phishing on this subject can continue. Also, the extension does not

necessarily improve merchants' awareness (particularly smaller merchants) of the need to meet the requirement. The industry may find itself no further forward as the extended compliance date draws closer.

Any addition of a stakeholder to the overall payments' ecosystem will increase the opportunities to either find security gaps or develop sophisticated social or programmatic attacks.

2.2.7 RTS Implications for Payment Service Providers

i. Fraud Detection

Ongoing fraud detection for the entire payment lifecycle is strongly advised; from pre-authorisation through to BNPL schemes. Fraud detection should be approached as a protective and dynamic operation across the entire payment ecosystem post-, during, and pre-transaction authorisation.

The ongoing protection of systems and services should include the detection of unusual patterns of behaviour. APTs (Advanced Persistent Threats) are designed for long-term exfiltration using stealth. Sophisticated methods of hiding APT malware will continue to create issues for easy detection of such malicious software using more traditional tools. EDR (Endpoint Detection & Response) tools and Network Threat Detection and Response are holistic technologies that are used as part of the expanded device ecosystem.

These systems are increasingly AI-enabled, putting hard-coded rules in their place as fraudsters increasingly hide behind the massive numbers of payments. Transactional fraud is more difficult to detect and can require a two-pronged approach that looks at synthetic identity indicators alongside transactional behaviour.

One of the issues that has held fraud detection back has been false positives. Modern approaches to machine learning, have shown a reduction in false positive results. Systems that continually 'autotune' from false positives are being hailed as a more adaptive and accurate use of the technology. Researchers at Wallarm, found a 96.07% false positive detection rate.[xxix] Companies such as Ravelin use rules along with machine learning to detect patterns of fraud to put this into practice; it had results of over 60% reduction in false positives rates.

'Machine learning focus is not on fraud losses anymore, it is about customer experience and the move to a frictionless user experience. A lot of our customers in the fraud space will tolerate a certain level of fraud, as customer experience is key. The balance between friction and fraud is the balance we work to get right. Verifying good identity and differentiating this first, then using this against the bad patterns of behaviour – in other words, we look for the good footprint first rather than looking for the bad behaviour.' – David Mirfield, Head of Product, Financial Crime and Risk, GBG PLC.[17]

A key point made during interviews was that ultimately, fraud detection was about risk management as much as security. As channels of payment become multi-jurisdictional and cut across varying channels, risk profiles can be aggregated; providing a way to manage complex payment ecosystems and security.

The LexisNexis 2020 True Cost of Fraud identified omnichannel payments as being a pain point. The report found that being able to

[17] Juniper Research interviewed David Mirfield, Head of Product, Financial Crime and Risk, GBG PLC in March 2021.

distinguish between legitimate customers and bots is becoming increasingly difficult and that 'those who use a layered solutions approach, as well as one that integrates cybersecurity, the digital customer experience, and fraud prevention efforts, experience fewer comparable fraud attacks, are better able to detect botnets and minimise customer friction and realise a lower cost of fraud.[xxix]

Omnichannel is a repeated noted challenge across reports and studies. Visa reports the use of AI in banking for fraud detection is increasing largely due to concerns about omnichannels involving mobile wallet and P2P payments. The main fraud areas of focus are identity verification/synthetic identity, bot attacks – mobile device infection leading to identity theft and hacked accounts and transaction monitoring.

'What we see at Kount is a 'heartbeat transaction,' whereas Equifax often sees a 'life event.' For example, you do not apply for a credit card every day, but you do buy coffee every day. Using these events and other behavioural factors such as how you use your devices, where you live, etc, are all behaviour patterns; the two pieces of the puzzle can be merged to prevent synthetic identity. There may be enough signals to link the physical and digital footprint of an identity. This can turn out to be a fraudulent identity: The challenge is to work out if it is legitimate or a thin footprint.' – Vikram Dhawan, Vice President and Senior Product Leader, Kount, an Equifax Company.[18]

ii. Merger of Home Working, Personal Devices, and Corporate Access

The COVID-19 pandemic has created a much larger service surface area by forcing the work from home movement that has allowed incorporation of a wider BYOD (Bring Your Own Device) remit for many organisations.

Personal devices and corporate access are becoming fuzzy and with that, login credentials, authorisation of payments, and corporate app access are becoming fuzzy. In a recent report, one-fifth of consumers were found to be using their work email or password to log in to consumer websites and applications such as food delivery apps and online shopping sites.[xxx] A zero-trust approach to access control can have positive ramifications for both corporate data breaches and payment security if enacted. Zero Trust Architectures need flexible identity and access management that can provide the verification needed at the right point in an access event. With a defence-in-depth approach that takes advantage of modern machine learning-based EDR and other network detection tools that augment dynamic IAM systems, the separation of personal authorisation mechanisms with corporate access can be achieved.

iii. Exemptions from SCA

Although the RTS states that PSPs must have mechanisms in place to detect possible fraud, there are no specifications with regard to the type of fraud solution that should be used. SCA is expected to be enforced regardless, unless PSPs conform to an additional set of requirements, which include the following:

Adoption of RBA (Risk-Based Authentication) mechanisms, such as via a fraud detection solution, implementation of 3D Secure 2.0 (or a possible combination of both) will allow PSPs to bypass SCA where the risk associated with the transaction is deemed to be low.

RBA must take into account:

[18] Juniper Research interviewed Vikram Dhawan, Vice President and Senior Product Leader, Kount, an Equifax Company, in March 2021

- Abnormal spending patterns and previous transaction history;
- Software or device abnormalities;
- Malware infection;
- Fraud intelligence in respect to known activities or patterns;
- Location of both the payer and payee.

Nevertheless, PSPs that do apply RBA must monitor and report recorded transaction fraud levels on a regular basis to the EBA. Where fraud levels exceed the exemption thresholds set by the EBA for two consecutive quarters, PSPs must enforce SCA on a strict basis until the reported fraud rate matches or falls below the designated threshold, shown in the table below.

Figure 2.2: CNP Fraud Rate Thresholds for SCA Exemption

Value	Fraud Threshold %
€500 ($580)	0.01%
€250 ($290)	0.06%
€100 ($116)	0.13%

Source: Official Journal of the European Union

COVID-19 has meant delays to the implementation of SCA, but social distancing measures have also meant that CNP has experienced a surge in use. One of the outcomes of social distancing has also been to increase the limit on contactless payments. In the UK this was increased to £45 and may be increased to £100 as per a consultation by the FCA (see below). This is in line with the PDS2 requirement that states in Article 63 that 'they may increase them for prepaid payment instruments up to EUR 500.'

The FCA in the UK is currently consulting on barriers that they believe will impact the success of Open Banking and UK payment innovation in general. The FCA is suggesting that amendments to the Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication are made. The consultation is due to close on the 30th April 2021.

iv. Implications

There has been a degree of uncertainty about the RTS and SCA. COVID-19 has exacerbated and already moving goalpost of implementation. New challenges to deal with the sudden spike in CNP payments and socially distanced contactless, as well as the increased use of apps to purchase food, has placed the remit of PSD2 under unexpected pressure. Cybercriminals have taken full advantage of this situation. It has been a time of monitoring to see how the regulatory bodies moved, as the pandemic shaped out. But fraudsters never sit on their laurels and have taken full advantage. A 2020 report from the European Central Bank found that almost 80% of the total damage caused by card misuse was down to CNP transactions.

FDP solution providers who are able to incorporate all the elements described in the minimum requirements for RBA will be preferred.

Some convergence between fraud detection and IT security elements including security awareness and zero-trust models, are likely to take place to meet requirements for malware detection.

'There will always be an appetite for vendor-led scores and scoring. But for organisations that have economies of scales and in-house experts, they will be empowered by using the same ML tools to create their own models.' – Robert Capps Vice President Emerging Technologies, NuData.[19]

2.3 The Fintech in the Equation

Fintechs continue at pace to seed the payments market with innovative solutions. The IoT market space and payments are providing new areas that fintechs can innovate into. Coupling the SCA requirement with IoT payments is a natural coupling for a fintech option. Security and privacy are other areas that fintechs could excel in; offering new pathways for partnerships with incumbent banks, and in doing so, offer a more secure payment experience. Also, by default, a fintech is digitally native; making it easier for fintech products to integrate FDP systems compared to big banks that may have complex and legacy core banking systems.

The resilience of fintech vendors came under scrutiny with the Wirecard debacle, which asks the question if certain fintech models are robust, as many fintechs were served by Wirecard, and must have impacted on fintech stability. In response, the FCA froze eMoney accounts and payment transactions handled by Wirecard.

The contactless digital payment opportunities afforded by the pandemic are not lost on fintechs, and new entrants and older fintech players, continue to enter and adjust to the space. Many of these fintechs are enablement platforms; bringing ecosystem layers together to provide new products and new ways of paying. This expansion of the payments landscape also offers cybercriminals opportunities, as new APIs connect and data (and money) flows across complex, interwoven systems.

2.4 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 bricks-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.[xxxi]

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.[xxxii]

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

[19] Juniper Research interviewed Robert Capps Vice President Emerging Technologies, NuData in March 2021

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 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 (eg PSS256) and the signature must be verified against a public key available on a public JWKS endpoint. In addition, or alternatively, mutual TLS should be established between the Provider and the RP.

b) Unauthorised modification of requests or token responses

Because authorisation codes and multiple tokens may be returned as part of the OIDC 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 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. (One example of how not to do this is in Apple's 'Sign In with Apple,' where user attributes are returned as unprotected query string parameters).

ii. API Authentication Security

Despite a delay in the ratification of the RTS 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 tokens (JSON web tokens, JWT), 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 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, 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 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 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.

2.5 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 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 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 2.3: Global Instant Payments Market Status

Source: Juniper Research

Awareness of instant payments by industry is at a high, with a PAYMNTS report showing that 85% of organisations have instant payments on their roadmap for implementation in the next three years.[xxxiii]

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 SMEs. 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 SMEs 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,

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

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.[20]

2.5.1 Fraud & Payments

Payment options are themselves creating dichotomies because of fraud prevention. Whilst in PSD2, CP rules have been derogated to allow a more seamless UX; 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 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 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, eg 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.[xxxiv]

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 mobile transactions, with money received via the app free to be spent immediately.

These same issues, ie the inability to respond to the demands of new payment schemes, will likely impact the rapid take-up of cross-border schemes, such as SCT Inst 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 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 (ie 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

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

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.[xxxv]

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' fraud, such as lost and stolen cards, 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.

ii. Further Protections Required

a) APP Fraud

A voluntary scheme to reimburse victims of APP fraud, the Authorised Push Payment (APP) Contingent Reimbursement Code, came into play in May 2019 and is expected to continue to 30th June 2021. The code has reimbursed over £89.2 million ($125 million) to thousands of customers since it came into effect.

The finance industry, even with a consumer protection mechanism that is voluntary, has a driver to protect against APP fraud. The financial sector is responding by improving consumer awareness of financial fraud; in the UK, this takes the form of the 'Take Five to Stop Fraud' campaign. Other initiatives to help reduce APP fraud include the 'confirmation of payee' checks. Next on the agenda is a system to look for fraudulent text messages which are often the starting point for an APP scam.

b) eWallet fraud

The European Payments Council report points out that targeted attacks on mobile device key stores unlock credentials, user interfaces and NFC controllers are all being used to target payment wallets.

iii. Fraud Detection Spend to Increase

As noted earlier, the real-time nature of instant payments will require the implementation of real-time fraud protection. Facilities such as 'confirmation of payee' and 'request to pay' on the recipient's side will undoubtedly be an additional layer of protection, although any move from a batch-based transfer scheme to one that handles individual transactions will inevitably require investment to prevent new fraud from occurring. In the consumer market, this demand will undoubtedly come

from P2P transfer and remittance schemes, given that eCommerce merchants are likely to favour card networks until instant payment schemes are well-established.

Juniper Research predict that spend on FDP solutions is expected to rise from $8.3 billion in 2019 to $9.9 billion in 2024, a CAGR of 3.7%.

2.5.2 Digital Identity & Fraud

Digital identity is increasingly perceived as the thin end of the fraud wedge. Get identity right and you have a good basis for further successful fraud detection, as the relationship between service and customer develops.

'There is very much a growing use case and a market for identity and payments. As payments become more digital and P2P payments accelerate, there is an additional need for identity-linked fraud mitigation. For example, with identity and fraud it is becoming a necessity for business to be able to trust within the digital world. Companies must be able to trust users during the onboarding process.' – Laura Barrowcliff, Head of Strategy, GBG PLC.[21]

i. Decentralised identity wallets

Juniper Research places a note on the use of decentralised, blockchain-based identity wallets that may be used to prove the identity of a person. While blockchain may be robust in design, the system at the point of the user/device may become an attractive attack vector to gain control over the otherwise highly assured identity. Once under the control of an adversary, this assured identity could be used to carry out fraud that is then difficult to detect.

2.6 3DS 2.0 (3-D Secure 2.0) & Biometric Authorisation of Transactions

Juniper Research biometrics will authenticate over $3 trillion of payment transactions in 2025, from just $404 billion in 2020. The report, however, found that whilst biometric capabilities will reach 95% of smartphones globally by 2025, only 35% of these smartphones will be used for making biometric payments in eCommerce in the same year.

3DS 2.2 has several minor updates on its predecessor. EMVCo[xxxvi] outlines them as:

- Enablement of PSD2 exemptions for SCA to be applied.
- New features to enable authentication for various payment scenarios including mail order and telephone order transactions:
- 3RI (3DS Requestor-initiated) payments – enabling a merchant to initiate a transaction even if the cardholder is offline.
- Decoupled authentication – allowing cardholder authentication to occur even if the cardholder is offline.
- Support for FIDO Alliance standards.

[21] Juniper Research interviewed Laura Barrowcliff, Head of Strategy, GBG PLC in March 2021

Figure 2.4: Uptake of 3DS2

Source: EMVCo Annual Report 2020

3DS2 looks like a stopgap measure whilst waiting for full PSD2 roll-out. Certain national authorities (including France and Germany) have decided to go down the soft decline route. A soft decline is a declined authorisation that can be reprocessed and is being used to de-risk non-compliant transactions during the transition period to PDS2 regulatory compliance deadlines. The soft decline is based on a new flag (ISO 8583 response code 'A1') for risky non-compliant transactions that allows a merchant to retry the transaction using a 3DS2 flow. This soft decline route is a temporary measure and indicative dates with associated amounts are:

- January 2021, only non-SCA transactions exceeding 1,000€ could be soft declined.
- February 2021, only non-SCA transactions exceeding 500€ could be soft declined.
- April 2021, all non-SCA transactions flagged as too risky by the issuer's TRA could be soft declined.

There are two significant benefits from 3DS2 implementation:

- Reduced consumer friction: Merchants have previously been reluctant to implement 3DS 1.0 on account of high-friction authentication challenges, which led to increased cart abandonment rates. In regions where risk scoring approaches are uncommon, this has meant that merchants rated losses from cart abandonment higher than the potential losses from fraudulent activity. The new protocol also ends the practice of static, password-based authentication in favour of OTP (One-Time Passwords, typically sent via SMS), KBA or OOB (Out-Of-Band) authentication, which may use biometric information or a separate authentication mechanism.
- Multi-channel implementation: The 3DS2 protocol is device agnostic, meaning it is suitable not only for web implementation for PCs, but also on mobile web and app channels. This wider implementation potential will mean that the system becomes more familiar to consumers and will ultimately lower cart abandonment rates.

2.6.1 Authentication Mechanisms

i. OTP (One-time Passwords)

It is likely that OTPs sent by SMS will quickly become one of the favoured authentication mechanisms for merchants implementing 3DS2. This is because SMS is the single unified standard for messaging individuals; the instant messaging landscape is fragmented, while SMS is typically more reliable than email.

The use of SMS will mean that a phone number will need to be registered with the user's acquiring bank which, in turn, should provide a proof of payment request for authenticity. Nevertheless, SMS is highly vulnerable to several attack vectors:

ii. Biometrics

SDKs that facilitate issuer apps to use a biometric for 3DS2 authentication may change the goalposts moving SMS text. Biometrics allow for more consumer choice, no ongoing text costs, and a nicer user experience than waiting for a SMS text code and then entering it into an interface. However, this is unlikely to increase the expected 35% of smartphones used for making biometric payments in eCommerce by 2025.

iii. SIM Swap Fraud

In this attack, fraudsters contact the victim's MNO and masquerade as the victim, claiming to have lost the original SIM tied to the victim's mobile number. Identity checks initiated by the MNO to verify the request are typically easy to overcome as the questions often involve information that can be gathered from the public domain, or social media.

Armed with a new SIM card, the fraudsters then trick the MNO into disabling the victim's card and activating the one in their possession. In this manner, OTPs are routed to the fraudsters; defeating the authentication challenge mechanism. For this type of attack to be successful it is important that the victim does not notice that his/her SIM has been deactivated. This means that the highest rates of attacks by fraudsters will be at night, when the victim is assumed to be asleep.

In 2021, Europol arrested a network of SIM Swap fraudsters, who are believed to have stolen over 100 million in cryptocurrency. The attackers targeted high-profile individuals This targeting of high-profile and famous people is a niche attack surface but one that is lucrative.[xxxvii]

iv. SS7 Vulnerabilities and 5G

Due to the fact that SMS was developed before the emergence of the commercial Internet, it should come as little surprise that the cross-network routing mechanism for messages, SS7 (Signalling System No 7), was not built with high security in mind. In effect, where fraudsters have gained access to the SS7 network, they have the potential to re-route any SMS messages to a destination of their choice. This means that OTPs intended to authenticate the victim can be routed to a fraudster's device; allowing them to defeat the challenge mechanism.

As 5G comes down the line, it is likely that migration will rely on this older protocol, with the result that vulnerabilities will be exploited by cybercriminals. In 2020, a talk at BlackHat, 'Back to the Future. Cross-Protocol Attacks in the Era of 5G' by Positive Technologies described how legacy security flaws in the SS7 protocol are a continued danger, and cross-protocol attacks are likely to take place.[xxxviii]

v. Malware

Malware designed to intercept SMS text messages has been around for several years, often part of banking Trojans. These have been widely noted on Android platforms and some complex malware, such as AceDeceiver, are starting to target IoS by using flaws in Apple's DRM system.

vi. Man-in-the-Middle Website Reverse Proxies

This form of attack is not just confined to SMS texts, but can be applied to most common second factor methods. It involves faking the target site which, when used, forwards and retrieves two-factor requests and responses to and from the target site; response tokens or session IDs may then be used by the hacker for their own use of the target site. Modlishka is one of the toolkits available for this hack.

vii. Dark Net and Pandemic Implications

The COVID-19 pandemic has seen a spike in online goods purchases, as well as app-based purchases of food for delivery. Fraudsters follow the money, and the dark net is still offering stolen data and cards, although a decrease has been noted. A SixGill analysis found that 45.1 million cards were placed for sale in the first half of 2020, a 41% decline from the 76.2 million offered on dark web sites in the second half of 2019.[xxxix]

Juniper Research therefore still anticipates that fraudsters will favour online attack routes and take advantage of protocol vulnerabilities and other MiTM methods of attack.

viii. Conclusion

Due to the aforementioned weaknesses of SMS used for OTP, Juniper Research would advise using alternative, better secured methods where possible.

In particular, event-driven authentication and step-up authentication should be part of a robust approach to payment transactions, which can include biometric or behavioural data.

In 2019, the Web Payment Security Interest Group, which has representatives from across industry, was formed as a working group of W3C. The group is looking to 'enhance the security and interoperability of Web payments.' The Group's chairs have representatives from EMVCo, FIDO Alliance and W3C.[xli] In a press release in November 2020, the Group stated that:

'As more merchants move online, especially since the start of the COVID-19 pandemic, and fraud attempts increase, EMVCo sees this collaboration with the FIDO Alliance and W3C as a major contribution to advancing secure web-based payments, while also simplifying the online payment process for merchants and helping to reduce friction for their eCommerce customers.' – Bastien Latge, Director of Technology for EMVCo.[xl]

ix. KBA (Knowledge-based Authentication)

The fact that KBA has been selected as one of the possible methods of user authentication is odd, given that passwords are no longer able to be static for extended periods. Static KBA can be easily gamed by fraudsters, as the amount of personal data posted on social media networks and Web 2.0 sites rises. A dynamic version of KBA improves on

this by using real-time generation of questions based on various data sources. Whilst dynamic KBA is a more secure option than its static counterpart, it may still have consumer pushback, as users attempt to remember the answers to (usually) financial questions about credit and card use.

Dynamic KBA can also have some drawbacks in terms of the questions and their relevance. A confidential industry source told Juniper Research that during an implementation of a consumer system that used dynamic KBA, pushback was recorded using an IQ Tag Management system. The users found certain questions difficult if not impossible to answer, an example being a question on credit card ownership from 15 years previously. The moral of the tale is to find the right balance of questions that are relevant but difficult to guess or where answers can be found using stolen data or social platforms.

Because of these drawbacks, Juniper Research does not believe that this mechanism will have great future potential in the market. We believe that other authentication methods, including biometrics, behavioural and risk-based are more likely candidates to take authentication into the mid-2020s.

x. Authenticator Apps

These applications generally use the TOTP (Time-based One-time Password) algorithm, which generates a new code every half a minute or so. Such codes have a window of a minute or so in which they are valid. One of the best known of these is Google Authenticator. Any TOTP application may be used with a site that supports TOTP as a second factor. To be secure, sites that use TOTP must limit the number of attempts at entering codes, or they can simply be broken by brute force.

Also, the secret shared between the app and the site must be kept secure as, once compromised, a hacker can use it to generate their own valid codes; this happened, for example, in the hack of Linode, a cloud provider, in 2015.

The main issue with TOTP is usability; transferring TOTP settings from an old to a new phone can be very difficult.

xi. Biometrics

Biometrics are commonly fingerprints, as used by smartphones or, alternatively, mechanisms such as voice prints, facial or iris scans. The latter have had some uptake among retail banks as a means of improving account login security over PIN numbers. Whilst there have been limited trials of biometric payment cards, thus far, these have been used mainly to try to improve contactless security/raise payment limits. While these have high levels of promise, they are still nascent at present. Juniper Research's report into the use of biometrics for payment's show promise in the use of biometrics going forward.

a) Vulnerabilities

Biometric data has the same level of vulnerability as any other type of credentialed data; it must be stored in a secure manner. This was evidenced in the BioStar 2/Suprema biometric breach, which exposed the biometric data (face, fingerprints, etc) of 1 million individuals on a publicly accessible database. The system underpins the AEOS access control system used by banks.[xlii]

The key issue with biometrics for authentication purposes is that the end-user is unable to refresh the data once it is compromised; a fingerprint, voice print or iris pattern stays the same, short of surgical

intervention. Juniper Research also expects that any compromise in biometric data will be difficult on the part of the consumer to legitimately claim. In the first instance, assuming a secure implementation where biometric data is stored in a SE, harvesting that data at scale becomes an issue. However, researchers have demonstrated many times how biometric data can be compromised, thus we must assume that there will be instances where incidents will occur. Vendors must therefore ensure that the most robust security measures for data security are in place.

2.6.2 Further 3DS Implications

The 3DS2 protocol is a data-intensive payment authentication mechanism as it functions most effectively when as much data about the cardholder as possible is shared between the merchant and the issuing bank. With this in mind, there are two key implications:

- A lack of transparency about the types of data collected about the cardholder, and how this data is handled outside the transaction process may, in the first instance, constitute a barrier where privacy-conscious individuals are concerned. More importantly, it may cause issues where the EU's GDPR is concerned. Indeed, the question here is about transparency; if consumers are unaware of the types of PII being collected, they may have cause to complain to those responsible for data processing. On the other hand, full transparency is a useful tool for fraudsters. If they know which datapoints are being used to risk-score a transaction, this gives them an opportunity to develop methods to game the system.
- The protocol is not backwards compatible with 3DS 1.x. This is important in the context of smaller merchants, which may not have the capability to collect and pass a high number of datapoints to the ACS (Access Control System), thus leading to a higher number of authentication challenges. In turn, this will discourage smaller players from using the system and lead to greater fragmentation in the market.

  However, 3DS2 reduces some of the friction associated with the inclusion of PSD2, SCA, for online payments. This is evidenced by data from Visa; showing that 3DS2 has reduced checkout times by 85% and cart abandonment by 70%.[xliii]

2.6.3 Next Steps & Regional Outlook

The online payments landscape is filled with consumer options that can be exploited in increasingly novel ways by cybercriminals. Juniper Research looked at the use of FDP software to 2025 for various global regions to help mitigate those threats.

As the last year has unfolded, the human in the machine has reared its head and the fact is that without understanding who you are dealing with, fraud will continue to escalate. Identity theft, synthetic identity, account takeover, and all of the other associated events that steal and expose personal data, feed fraud.

Fraud prevention is not a point solution. A 360-degree multi-lateral approach is needed to stem the flow of money out of legitimate hands into the bank accounts of fraudsters. Every touch point across a system and the APIs that handle the calls in between need to be hardened in a way that does not impact the user experience. This fine balance requires a socio-technical solution.

As far as regional variations are concerned, whilst payments rails are often shared across world platforms, the mechanism of regulation may

differ. The US payment regulations and infrastructure. The SCA may have originated from PSD2 but the EMVCo's 3DS2.2 is being used to achieve the requirement. Open Banking, originally an EU PSD2 initiative, has found a strong home in the UK and is now finding footholds across a global marketplace.

Regulations are increasingly touching a global audience because of the globalisation of eCommerce and payments. A regulation or initiative may begin in one continent, even one state (as in the CCPA [California Consumer Privacy Act]) but have far-reaching repercussions for retailers selling globally. China is unique and has embraced a mobile-first approach to payments, with the majority of citizens using WeChat Pay or Alipay. New payment rules in China may change this landscape in coming years. These anti-monopoly rules, that are still under review, mean that non-bank payment processors meeting certain limits could be subject to regulatory warnings.

However, whichever country a payment begins in, the same fraud challenge permeates the whole market.

Identity networks may hold the key, the principles of which are based on flexible identity data checks that work using a Zero Trust approach. Persistent identifiers may not be needed in payment systems, and exploration of alternative, no-account, ways of taking payment should be expanded. Open Banking offers the opportunity to perform this no-account transaction by offering an already KYC-checked 'identity' to a relying party, as well as providing payment rails. Open Banking could also offer a RTS approach that is user centric, bank validated, and using the right connectors, relying party friendly.

As we deliver customer-led experiences that traverse systems and place them as a central pivot of choice using Open Banking, we must also deliver the equivalent security. This requires a multi-pronged approach. Open Banking initiatives deliver innovation opportunities, but also open up systems to further cybercrime. Several companies interviewed as part of this report reiterated that no one solution will fix the fraud issue in payments; a multi-layered approach is needed.

'Reducing customer friction and keeping on top of new threats is where machine learning becomes essential. New rules could be added by experts, but you end up with thousands of rules. ML lets you organically add in new controls, but as the landscape changes, you can adjust the model by weighting the model to reflect this. The use of unsupervised machine learning, for new risk areas, lets you focus on new unusual patterns. Building a system that is efficient in targeting the known risks but gives you the ability to also focus on the unknowns is where machine learning excels.' – David Mirfield, Head of Product, Financial Crime and Risk, GBG PLC.[22]

Securing all fronts is essential to close off these threats. To this end, Juniper Research forecasts that application of traditional FDP software will continue to increase to 2024 at a CAGR of 3.7%. Securing the system as a whole, for all the facets of modern digital payments, is the key challenge for 2024.

[22] Juniper Research interviewed David Mirfield, Financial Crime and Risk, GBG PLC in March 2021

3. Online Payment Fraud: Segment Analysis

3.1 Introduction

Cybercriminals are nothing if not inventive, which has been demonstrated repeatedly in many segments. This fact was repeated throughout our discussions with vendors, many of whom stated that cybercriminals are highly reactive; changing tactics to suit the environment. The COVID-19 pandemic has shown this to be the case, with vendors finding that fraudsters effectively 'followed the money;' finding new mechanisms or adjusting existing ones to fit the new social distancing measures and uptick in digital transactions.

Track records in the payment fraud area have shown that for every payment transaction, there is an equivalent type of fraud. In this section, we pull out three segments and identify how payment fraud impacts these up to 2025.

3.2 Banking & Money Transfer

In April 2020, a notice from the IC3 (Internet Crime Complaint Center) stated that between January 2014 and October 2019, the organisation received complaints totalling more than $2.1 billion in actual losses from BEC scams.[xli] The COVID-19 pandemic is a demonstration of how BEC fraudsters adjust focus to execute fraud, the latest drivers for BEC fraud being in the form of PPE purchases; the FBI announced that multiple incidents involving state government agencies purchasing PPE ended in wire transfers of funds to fraudulent brokers and sellers in advance of receiving the goods.[xlii]

Although all business is at risk of financial losses due to BEC, higher-worth companies are likely to be targeted as higher gains can be made. Targeting involves a mix of surveillance, grooming of key employees (including at C-Level) and sometimes technical intervention, including email account takeover or malware infection.

Similarly, government benefits have offered opportunities for fraudsters. In the UK, for example, the Universal Credit benefit scheme saw a massive spike in claimants shortly after the first lockdown was announced. Around 1.5 million new claims were made in the month to 9th April 2020. Shortly after, investigations showed that around £1.5 billion ($2.1 billion) was lost to fraudulent claims. Most of these were attributed to organised crime groups and individuals taking advantage of the lower assurance of identity checks required in an effort to process the increase in claims during a difficult time for the individual. This ability to accept a certain level of fraud within a given context was discussed by Robert Capps, from NuData:

'Payment fraud and cybercrime are a 'pest' that feeds the livelihood of a certain group of people, as long as there is sustenance for that group, they will continue to do what they do. There was no cybercrime in 1982 and little in 1992. Probabilistic technologies leave room for failure. There will always be some level of attack on the system or the consumers themselves. The industry is working towards harm reduction and mitigation of the most egregious vulnerabilities. Cybercrime will never be zero because the cost to achieve that level of reduction is too great. The financial and consumer experience impacts always outweigh the risks. It

is about risk reduction, not risk elimination.' – Robert Capps, Vice President Emerging Technologies, NuData.[23]

The techniques attributed to banking and money transfer cover the spectrum of attack vectors, but this usually starts with social engineering and in the case of benefit fraud, poor KYC processes. For example, credential exposure, via spear-phishing can lead to an APT. The fact is, the ecosystem for payments is highly connected and multichannel, which plays an ever-increasing part in providing the mechanistic opportunities for nefarious elements in systems and services. This mix of behaviour manipulation through social engineering, in a matrix-like payments landscape, provides the perfect breeding ground for sophisticated cyberattacks to develop and persist.

3.2.1 Key Challenge: Advanced Persistent Threats

APT methodologies continue to be a favourite way to install fraud bots, exfiltrate data, and perpetuate financial-based attacks. Research from FireEye Mandiant concludes that, in terms of the current attack landscape, 'more attackers can do more things in more diverse environments.' The report also notes that cybercriminals are looking towards novel ways of monetising their criminal activities, including targeting corporate reward systems to steal gift cards that are then resold or used to make direct purchases.

In terms of APT infection, the FireEye report confirmed that phishing was the most prevalent method used to gain initial access to a target organisation prior to infection. The researchers did, however, find that dwell times have reduced since the first report back in 2012. Internal incident detection times have improved from 50 days to 30 days in 2019. The researchers put this down to improved detection methods.

A recent example of an APT group targeting fintechs and KYC processes, is Evilnum. Unlike many APT actors, Evilnum is avoiding the direct phishing route into an organisation and is instead using KYC processes to circumvent security. Spear-phishing, however, is part of the overall attack chain. The end result is infection with the RAT (Remote Access Trojan), known as PyVil RAT, designed to log and steal credentials, as well as exfiltrating other data of interest.

Security vendor CyberReason has analysed the PyVil RAT infection; finding a sophisticated multi-part execution of code.[xliii]

Various stages of download and dropper installation are performed; this includes an initiation via an archived LNK file that pretends to be a PDF document, but includes several spoof identity documents, typically used for a KYC process, eg utility bills, driver's licence photos, etc. Continued install events include the use of 'droppers' and schedulers that eventually lead to connection to a command-and-control centre. An obfuscated RAT is eventually downloaded and executed. The PyVil RAT has a number of functionalities including:

- Keylogger
- Running cmd commands
- Taking screenshots
- Downloading more Python scripts for additional functionality

[23] Juniper Research interviewed Robert Capps Vice President Emerging Technologies, NuData in March 2021

- Dropping and uploading executables
- Opening an SSH shell

Figure 3.1: PyVil RAT Attack

Phase	Example
Initial installation	Spear-phishing link LNK file masquerading as a PDF.
Analysis of system and detection evasion	Sophisticated communication with remote command and control centres, with dynamic re-encryption of malware.
Obfuscation for evasion	PDF used to hide LNK functionality. Uses modified versions of legitimate executables to evade detection. Code obfuscation to prevent interception of the payload using existing tools. Locates existing AV tools.
Activation of malware for target.	User execution. Windows Command Shell. JavaScript.
Privilege escalation	Use of scheduled task events.
C2C	Over an encrypted channel.
Data exfiltration	Credentials from password; stores/browsers/OS credential dump; screen capture.

Source: Juniper Research

One thing is clear, modern cybercrime is not a one-stop shop and it often requires teamwork for successful execution. Campaigns involve meticulous surveillance, sometimes including grooming employees, complex code modules that provide remote control and stealth-enabled features.

The breakdown of the attack reveals several flaws in victims' security protocols:

- Lack of security awareness training; spear-phishing being used to initiate attacks.
- Endpoint security was ineffective at detecting malware installed on machines. The APT was designed specifically to use modified versions of legitimate executables to trick AV tools.
- Privilege escalation was a key feature of the attack. This is difficult to contain once the attack begins, but AI-based pattern recognition could have been used to detect unusual behaviour.
- A Command and Control centre was an important part of the infection/exfiltration chain.

3.2.2 Key Challenge: Open Banking & Multi-part Attacks

Whilst PSD2 has tightened up areas like authentication, other attack vectors have been created by Open Banking APIs. Multi-part cyberattacks based on phishing, and spoofed Open Banking APIs are a threat. A multi-part threat chain involving the use of omnichannel entry points, such as social shopping sites like Instagram, could pave the way. An Open Banking chain of events from social site, to spoof eCommerce site and spoof Open Banking call, could result in a socially engineered API attack surface. A trojan designed to replicate an Open Banking flow may come down the line.

Although the need for greater implementation of real-time fraud prevention technology has been discussed in section 2.3, it is inevitable that fraud prevention tools cannot be 100% effective. Fraud prevention must have a multi-layered approach; it is here that money transfer fraudsters have identified a missing layer in some banks, either integrated with money transfer services or, indeed, providing transfer services directly.

For banks, the move to digitise services and participate in the era of Open Banking means that emphasis on security best practices must be greater than ever. Where previously the customer and their access to banking services was under the bank's control, this is no longer the case because of third-party service integrations and APIs for PISPs/AISPs. Service providers must therefore be acutely aware of the fact that the attack surface for fraudsters is now larger than ever. Therefore, the spread of powerful Open Banking APIs offers a potential gateway to significant fraud, especially if the 'trusted' third parties are compromised or MitM attacks are performed on poorly implemented protocols. This will result in the mechanisms proposed under FAPI, such as Mutual Authentication TLS, being rendered ineffective. A focus on the connection points between Open Banking APIs and the relying parties using the system, along with the token exchange flow, should be hardened and PEN tested regularly – this includes ensuring that any token longevity vulnerabilities are addressed.

With banks often relying on legacy systems and in-house development processes, keeping pace with agile fintech players and challenger banks is not easy. Legacy IT has been pulled out as an issue by Checkpoint, which states that: 'Legacy security tools are not designed for the dynamic, distributed, virtual environments of the cloud.'[xlvi] As a result, pressure to develop competing services can sometimes mean that normally robust digital security for longstanding services becomes much less so as new services are rolled out to customers.

Techniques that work to mitigate fraud will become part of a wider ecosystem of FDP. Like the multi-part attack vectors to which cybercriminals are turning, the industry must look to apply the optimal anti-fraud technique at the right stage of the payment lifecycle.

The underlying message is that banking service providers must view the market landscape not just as a competitive environment, but also one where best practice to evade fraud can be learned. Collaboration between vendors shows that the whole is greater than the sum of the parts where fraud prevention is concerned. It is therefore prudent that competitors' common processes and service features are routinely examined in the context of fraud prevention and digital security. As Robert Capps told Juniper Research:

'SCA and 3DS2 help reduce fraud in those areas, but this then drives fraudsters into other areas. Fraud is not just a technological issue, it is a society issue too. Prosecution is a key part of managing cybercrime. I watched $50 million in annual fraud volume drop by 50% after targeted prosecutions.' – Robert Capps, Vice President Emerging Technologies, NuData.[24]

3.2.3 Key Trends & Outlook in the Financial Sector

Fintech companies continue to innovate to meet exceptional customer needs in a digital realm. Fintechs have shaken up banking, and there

[24] Juniper Research interviewed Robert Capps Vice President Emerging Technologies, NuData in March 2021

seems to be no way back. Consumer banking, in particular, has seen fintechs make inroads; developing new banking products such as aggregation apps using Open Banking to bring multiple financial accounts together under one hood. Banking APIs and the expansion of real-time payment systems build real competitive edge when done well and in line with a great customer experience. Traditional banks, however, are making moves to push back. Some banks and FIs are creating either strong partnerships or even acquiring fintechs to add these innovations to their product portfolio. An example is the purchase of Open Banking aggregator platform Finicity by Mastercard. However, fintechs have innovated by taking short-cuts in some areas. This includes robust and extensive KYC. This has held certain product areas back from the reach of fintechs, and certain companies have been held up by regulators for not using robust KYC processes – better KYC afforded by more dynamic, API-based, document checking services, if done well, could move fintech reach into the traditional banking space. As mentioned in section 2.4, the Wirecard, debacle, whereby 1.9 million euros ($2.3 billion) went 'missing,' opens a debate on having not just KYC, but also KYB (Know Your Business).

On the topic of the CX (customer experience) – 'Will the industry be able to push fraud down any further? Given the proliferation of use cases, there is very much of a lifecycle approach now to fraud management – 10 years ago, it was about getting rid of fraud altogether; more recently it was about how to balance fraud against CX. Now, with the most sophisticated clients, a new opportunity is rising where it is 'nice' to manage their own fraud, but it is imperative to influence the issuers to accept more transactions. This is about fraud management going through three evolutionary phases, 1.0, 2.0, and now 3.0. Fraud 3.0 is about making sure you tolerate a level of fraud, whilst providing a good customer experience; it is very competitive out there, and if a consumer cannot get what they want out of an eCommerce setup, they will go elsewhere.' – Andrew Naumann, Product Management, Cybersource (Visa).[25]

Despite potential integration problems from legacy, or isolated, software systems, the movement to API-driven account service provision in major digital commerce markets should alleviate some of these issues, as banks increase their digital investment.

There were many fintech M&As (Mergers & Acquisitions) in 2020, included purchases of Open Banking TPPs (Third-party Providers), such as Plaid (Visa) and Finicity (Mastercard). The Plaid acquisition ended in failure because the DoJ (US Department of Justice) was concerned over anti-monopoly issues. However, the positioning of Open Banking capability within a wider ID network could help banks position and monetise their use of Premium APIs, as well as improving consumer experience and offering retailers real-time payments.

Behavioural biometrics and other types of authentication can also be used in an identity system that supports event-driven authorisation. Some API-based identity services can be used to apply contextual rules that use dynamic data (often behavioural) to authorise transactions. In a similar manner, event-driven KYC can be used to perform regular user identity verification.

[25] Juniper Research interviewed Andrew Naumann, Product Management, Cybersource (Visa) in March 2021

3.3 Remote Goods Purchases

The main threat to merchants selling digital or physical goods is CNP (Card Not Present) fraud, and this is unlikely to change for some time, given the continued number of data breaches that occur every year. The COVID-19 pandemic has only compounded this situation, with social distancing meaning that people have taken to the Internet to buy everything from groceries to garden chairs. The use of eWallets, as predicted by Juniper Research has been expedited by the pandemic, with consumers using wallets to fit in with social distance practices in shops. However, key challenges are either bedding in or emerging that will impact on the remote goods area.

'There was a significant uptick in digital transactions in eCommerce, at nearly 20% growth during COVID-19. Furthermore, 38% of consumers globally intend to spend more in the next 12 months. This increased activity will be most prevalent in the areas of online banking and digital purchases of goods, including online orders for groceries and food. The channels for online purchases are varied across numerous device types (laptops, tablets, mobile phones, connected devices, etc), which require businesses to employ a combination of device recognition and device intelligence, behavioural analytics and other contextual data as part of the overall risk assessment. Using this wide assortment of data attributes, Experian's solution can see if the transaction is a healthy one or not. We have the ability to collect this data via APIs, SDKs to be integrated into mobile apps as well as via browser interactions.' – David Britton, VP Industry Solutions, Experian.[26]

'We have to meet client needs across the entire payments' spectrum both pre- and post-transaction, eg at the point of login to a mobile app, and post-transaction chargebacks, as well as points that fit with regulations such as PSD2.' – Andrew Naumann, VP Product Management, Cybersource (Visa).[27]

3.3.1 Key Challenge: Synthetic Identity

SIF (Synthetic ID fraud) continues to evade detection. These contrived identities are often made up from a mix of real personal data and invented information; this can make them much more difficult to detect. A 2020 Payment Fraud Insights piece from US Federal Reserve, identified certain drivers of synthetic identity, including the increase in the already vast amount of personal data available from data breaches. One of the key issues found by the researchers was the use of 'piggybacking' whereby a fraudster adds a synthetic ID as an authorised user to the account of a legitimate user with a good credit rating. This allows the fraudster to generate a rapid positive credit file that is real enough to help meet the requirements of a KYC process.[xliv]

The paper continues by saying that traditional rules-based fraud tools are ineffective at detecting synthetic identities, with one study from ID Analytics estimating that 85% to 95% of likely synthetic identities were missed when using traditional anti-fraud methods. Certainly, more flexible approach afforded by AI-enabled fraud detection, especially tools that utilise multiple data sources, can be applied to resolve this issue.

[26] Juniper Research interviewed David Britton, VP Industry Solutions, Experian in March 2021.
[27] Juniper Research interviewed Andrew Naumann, Product Management, CyberSource (Visa) in March 2021

i. Detection

Detection of SIF is an extremely difficult task; indeed, this is one of the reasons behind its increasing popularity in the fraudster community. Once an account has been created using the fake ID, behavioural analysis will not normally flag any anomalies, as the KYC process has been successfully fooled. Even in cases where an FDP solution detects something out of the ordinary, because the account identity is considered genuine, fraudulent purchases will most likely slip through the net, as long as the fraudster is able to re-verify the account identity.

It is therefore critical that eCommerce merchants focus not only on transaction fraud detection, but also on new account fraud.

'Synthetic identities are about having a layered understanding of fraud and the ecosystem. What is the right identity check to do first? Often, synthetic identities look like a real person, but it may be a true identity, sold on, rather than synthetic – for example, an oversea student may have an identity for three years but then sell that on when they leave the country: That ID looks like a synthetic ID but it is different in terms of detection. The challenge is this is not a one-size-fits-all model. You need to call out to the right checks to ensure you catch all the variants of synthetic ID fraud and encapsulate the ecosystem to target the right data sources.' – David Mirfield, Financial Crime and Risk, GBG PLC.

One way to minimise the threat of synthetic identity is to create identity accounts that have high confidence levels met during registration and in use.

Verified identity can be achieved using an API, platform, or service:

These APIs, services or platforms link to third-party services that provide identity checks, AML scoring, and other fraud checks. The registered identity account can also be linked to robust authentication measures.

Furthermore, rules can help to modify the behaviour of the service both during registration and in identity consumption by replying parties to provide continued monitoring and checks.

The above verified identity offerings can be augmented using biometric behavioural analysis. The manner by which data is entered when opening accounts, and the way in which the device in question is used, or held, can give valuable data as to whether information is being input by a genuine user or a fraudster. This data can be made more powerful when integrated with other identity metrics collected by players referred to above.

- Activity history: Most people have a history of financial behaviour, email and phone accounts, as well as social media usage. This data can be cross-linked to build a score that gives a measure of the likely real existence of the individual. Those with lower scores could be offered reduced credit or be subject to more intense scrutiny.

Vendors should choose to engage with players which maintain significant databases of digital identity metrics and are able to evaluate a number of different markets and channels. This will help detect tell-tale signs of a faked identity.

'The market has seen an evolution in the case of identity verification that is applicable to payments. We are seeing a strong convergence of these ID requirements as associated to payments and transactional risk. Experian is in a unique position, as we have strengths across both of

these functional requirements.' – David Britton, VP Industry Solutions, Experian.[28]

ii. Zero Trust Payments

An alternative, that can avoid a merchant needing to create their own verified identity is to use a 'zero trust payment approach.' This allows a merchant to use an existing verified identity and/ or perform on-the-fly checks against user data, without the need to store these data. For example, an ID Network could provide the means to interact with an Open Banking API to 'piggyback' on the KYC performed by the bank. The user authenticates using their bank and accompanying credentials (which could be a biometric) – this is both validates the transaction and has the potential to include RTP capability.

3.3.2 Account Takeover

'Account takeover is insidious because I can phish your account and I can then use your reputation. It is very hard to detect account takeover fraud, you cannot tell if a user is phished until it is too late. If there is a customer in good standing with an account at a merchant, then the fraudster can get at the vetted account and the customer's good reputation. This is more than just stealing a credit card; fraudsters use a reputation to fly through the process of KYC or other checks – the fraudsters move upstream – using machine learning-enabled tools allows you to check things like IP address and other variables during a transaction to help stop the account takeover fraud in real-time.' – Andrew Naumann, Product Management, Cybersource (Visa).[29]

The Verizon Data breach investigation report for 2020 found that 80% of breaches were due to brute force, cracking, or the use of lost or stolen credentials in credential stuffing attacks or similar.[xlv]

'Fraud is happening in bursts: As data breaches and stolen credentials are putting data out in the open. This opens a window to allow fraudsters to milk this data to perform fraud. Microsoft plots curves to show the breach then a huge surge of fraud, then it dies down, not because fraudsters stop trying, but because the defences work. Then the fraudsters give up. The interesting part is not the surge, but that they provide new vectors – the current one are money mules, perhaps because of the economic situation caused by the pandemic, as there are a lot of people in financial pain.' – Anand Oka, Partner Group Program Manager, Microsoft[30]

Account takeover is a point of inflection in payment fraud, effectively providing means to perform the 'piggybacking' as outlined in 3.3.1, or to completely take over reward accounts and other reputational elements of an account. Being able to tease out if a credential use is a bot or a human is an essential step in fraud detection and prevention.

As Robert Capps of NuData told us: 'Focus on payment security is around context. Is the transaction human or a computer interaction with the service? Is it the right human, Ms X or someone who has 'Ms X's' credentials? If its non-human, is it a bot? Is it good automation or bad automation? Good automation could be a financial service aggregator – this is wanted automation but may have an unwanted side, eg an account

[28] Juniper Research interviewed David Britton, VP Industry Solutions, Experian in March 2021
[29] Juniper Research interviewed Andrew Naumann, Product Management, Cybersource (Visa) in March 2021
[30] Juniper Research interviewed Anand Oka, Partner Group Program Manager, Microsoft in April 2021

validation attack happens through those services.' – Robert Capps Vice President Emerging Technologies, NuData.[31]

3.3.3 Omnichannel Fraud

Where physical goods are concerned, these purchases will typically be for high-value goods, such as consumer electronics, which are easy to purchase and resell for illicit gain. The merchants most likely to be targeted are those operating an omnichannel sales strategy, where goods sold online can be picked up in-store. Friendly fraud has seen an uptick during the pandemic. ACI Worldwide told Juniper Research that:

'During the pandemic, the sheer volume compounded friendly fraud. In the first lockdown, we saw a 27% increase in friendly fraud, probably due to ticket refunds and concern over the stability of companies. On the fraud side, saw real increase in click and collect fraud – with a 7% fraud attempt rate. Other delivery channels only saw about 4%-6% fraud rate attempts. In Europe click and collect was suspended due to the pandemic, which might explain why it did not spike further.' – Amanda Mickleburgh, ACI Worldwide.[32]

Having to meet the massively increasing transaction volumes across digital channels, seen during the pandemic, has provided ample opportunities for fraud. Friendly fraud is just one aspect of this but perhaps offers an insight into the complex nature of payment fraud. How to tell the difference between non-fraud events, friendly fraud, and malicious fraud is becoming difficult because of increasing volumes, expanded digital channels, multi-part channels involving digital/physical (such as click and collect) and new modes of fraud. These variables require a level of intelligent analysis only available by using smart technologies, such as machine learning.

A GBG PLC 2020 report found that explored how the financial services sector is tackling fraud, found that 96% of FIs are looking AI-enabled technologies to help improve fraud detection:

'There is a greater demand for AI and machine learning, as 96% of respondents show a desire to tighten and improve fraud detection for their customers using these latest analytics approaches, which are described as promising.'[xlvi]

'Omnichannel was cliched in 2010 but offering multichannel fraud support and protection across mobile and online in now more important than ever. Jumping through escalation and verification methods, all in one place, with easy to manage interfaces, is a big differentiator for FDP tools.' – Eric Leiserson, VP Research and Marketing, IDology.[33]

'Account takeover can happen in one of two ways: Compromising login credentials or a fraudulent entity creating an account from scratch. It is important to work across the customer continuum, from initial account creation to login, to account management and payments, you need to protect all points against account takeover actions, and across all device types.' – Vikram Dhawan, Vice President and Senior Product Leader, Kount, an Equifax Company.[34]

[31] Juniper Research interviewed Robert Capps Vice President Emerging Technologies, NuData in March 2021
[32] Juniper Research interviewed Amanda Mickleburgh, Director Product – Merchant Fraud, ACI Worldwide in March 2021
[33] Juniper Research interviewed Eric Leiserson, VP Research and Marketing at IDology in March 2021.
[34] Juniper Research interviewed Vikram Dhawan, Vice President and Senior Product Leader, Kount, an Equifax Company, in March 2021

Payment service providers and merchants must continue to put robust structures in place to reduce the risk of the various types of identity fraud. FDP investments, along with more stringent identity verification during KYC, should focus on reducing synthetic identity and other misuse of identity accounts, including hijacking/account takeover/credential stuffing.

AML and KYC processes must meet the balance of robust identity checks, whilst ensuring that the UI/UX remains a frictionless. This is achieved using various techniques in UI/UX design, coupled with smart technology, such as behavioural analytics, etc. The use of event-driven authorisation and AI-enabled AML checks is another area to explore to prevent exploitation of existing relationships.

3.3.4 Key Challenge: Omnichannel Security

Juniper Research found that remote payments for digital and physical goods will exceed $5.6 trillion by 2025. This is facilitated by enhancing the customer experience by offering multiple ways to make purchases. In doing so, the omnichannel experience becomes an omnichannel security challenge. Cybercriminals map their strategy to the payment mechanism on offer.

David Britton of Experian identifies this customer expectation of usability and choice of channel as a key challenge in the future of payments:

'Experian recently conducted a study that found 55% of consumers have higher expectations of a good experience in a digital platform than before the pandemic. Digital traffic is not going down. In reports pre-COVID, consumers wanted visible signs of security. Now, whilst security is still top of consumers' mind, they are also eager to have strong and invisible methods of security where they do not need to be involved.' – David Britton, VP Industry Solutions, Experian.[35]

The challenge is to make the robust authentication methods usable, and to ensure that all touchpoints are hardened, including account recovery on all channels. This challenge will be compounded as digital assistants-based purchases increasingly enter the channel. Social media shopping opportunities, like Instagram Checkout live shopping, should be included in omnichannel security support. This type of experience can open up opportunities for malicious apps that take advantage of social engineering. Finding the balance of invisible security across multiple channels can be achieved using intelligent anti-fraud detection capabilities coupled with background ID checks within a zero-trust payment mode: Weaving in security on all possible channels whilst maintaining a seamless and frictionless user journey, requires holistic design thinking.

3.3.5 Key Trends & Future Outlook in eRetail

Reduced friction has always been the ideal goal of online transactions. But getting the balance of frictionless transactions coupled with security is tricky. A Microsoft December 2020 survey on cart abandonment and SCA, shows some interesting results:[xlvii]

- Authentication success rates (excl the UK) are 76% for web based and 48% for app based (mobile and gaming console).

[35] Juniper Research interviewed David Britton, VP Industry Solutions, Experian in March 2021

- Authentication abandonment rates (excl UK) are only 14% for web based and 25% for app based; suggesting customers are not yet comfortable with strong customer authentication.
- Challenge rates (excl UK) are 72% for web based and 73% for app based.

The implications of this are that there is still some way to go to meet the potential of SCA, including optimisation of authentication and consumer acceptance to improve acceptance.

'Where SCA is not a requirement but customer experience is, risk-based authentication can help reduce friction. In Europe it is a regulatory path, in the US and Canada, it is an economic path, but in either case, risk-based authentication meets the needs.' – Vikram Dhawan, Vice President and Senior Product Leader, Kount, an Equifax Company.[36]

i. Conclusion

There are a number of factors driving payment transaction losses across industry. Payment fraud, cart abandonment as SCA is enforced, increasing synthetic identity and omnichannel opportunities for cybercrime, all conspire against online and remote payments. Juniper Research believes that retailers will lose $16.5 billion in 2019 to $27.4 billion in 2024.

Behavioural and event driven authorisation can enhance security across omnichannel payment options. The use of solutions to minimise the friction impact of SCA and 3DS, using smart decisions based on AI analysis of multiple data points, will help alleviate the friction whilst increasing the security. The changes to limits on purchases could be used as a positive way to minimise friction when used in combination with AI/ML enabled anti-fraud solutions.

Ultimately, the payment network must be viewed as a cohesive and interconnected payment's rail, and the human touchpoints of this cannot be missed out of any security strategy. The use of zero-trust payment principles; using an existing KYC-checked identity, but performing on-the-fly anti-fraud checks using intelligent technologies, has to be an integral part of payments. Security requires pragmatism. But in a world where engaged and educated consumers are becoming the norm, this pragmatism requires flair in design and tooling. AI-enablement of payment rails is available and, when implemented in the right places with the right rules of engagement, it can remove friction and increase security.

David Briton of Experian sums up the challenges of the industry as follows:

'It is (the challenge in payments) going to be about how you sustain the operations in the new digital world. As consumers have higher expectations around their growing digital experiences, businesses are applying more advanced analytics and automation to handle the requests. We are seeing increased staffing around digital support to handle anomalies in those processes. All this boils down to achieving the ability to stave off the threat vectors which will continue to go through the roof, whilst balancing the lack of friction expected by today's consumers.'

[36] Juniper Research interviewed Vikram Dhawan, Vice President and Senior Product Leader, Kount, an Equifax Company, in March 2021

– David Britton, VP Industry Solutions for Fraud & Identity Management, Experian.[37]

FDP solutions can mitigate fraud from analytics across multiple datapoints. In the complex payments ecosystem across multiple channels, this capability is essential. Juniper Research therefore believes that FDP solutions should be viewed as an essential component of payment ecosystems playing an integral role in a defence-in-depth approach that augments other measures, such as tokenisation and anti-phishing capabilities.

What is clear following this analysis, is that the scale of potentially lost revenue, either through false positives, costly manual reviews or chargeback costs, is substantially greater than the cost of robust FDP solutions. Service providers must therefore focus on highlighting the essential benefits of identifying genuine transactions, as opposed to the upfront costs of an FDP solution.

3.3.6 Machine Learning

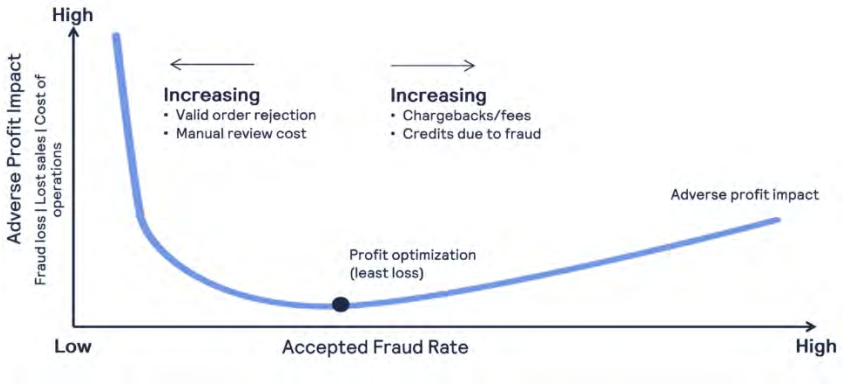
The application of machine-learning algorithms within anti-fraud solutions for payments is now an established technological approach; replacing the older, rigid, rules-based, algorithms. Machine learning-enabled platforms can manage the vast transaction volumes, the industry is seeing, especially during the pandemic. Also, the very nature of these smart technologies means that these extra data give the algorithms the information needed to adjust as new patterns of attack emerge.

Talking about the evolution of fraud management from a hard rules-based 1.0 version to the current dynamic AI-enabled platforms in V3.0 of fraud management, Andrew Naumann of Cybersource told Juniper Research:

‘There were three waves of fraud management. A fraud management 1.0 approach could not cut it because it delivered high rejection rates. If there is a risky transaction you cannot make a systematic decision, it could take hours for a human to check it. Fraud management 2.0 brought into play balance of the costs of fraud against aggressive rules. Version 2.0 resulted in false positives and loss of good transactions to achieve fraud reduction. A fraud management 3.0 approach brings in the internal costs to create a fraud deterrent: Fraud rate tolerance vs cost to business in rejecting orders and finding this balance, and the sweet spot of fraud acceptance vs cost of false positives. As merchants have embraced new customer norms and expectations of multiple delivery channels, this has introduced new levels of risk. This changing landscape makes fraud optimisation tricky. Because of multiple use cases, channels, and large CNP volumes, the use of machine learning to achieve this balance is needed.’ – Andrew Naumann, Product Management, Cybersource (Visa).[38]

[37] Juniper Research interviewed David Britton, VP Industry Solutions, Experian in March 2021
[38] Juniper Research interviewed Andrew Naumann, Product Management, Cybersource (Visa) in March 2021

Figure 3.2: Goal Revenue Optimisation Fraud Management



Source: Cybersource

FDP as an AI-enabled, cloud-based service, provides an affordable solution that can utilise machine learning, data analytics, and provide predictive models 'as-a-Service.' FDP products are often multi-capable and cover the lifecycle of fraud from detection and prevention to investigation. While the payment fraud market is buoyant, intelligent systems like FDP offer a way to balance the risk of remote CNP payments.

The proper application of machine-learning techniques in the fraud detection model offers an additional layer that can provide crucial automation and risk analysis. Adaptive analytics is an area of fraud detection that has great benefits. This technique allows real-time updates from fraud analysts to improve the accuracy of the FDP.

'It is important to ensure that the business has the appropriate framework where you execute machine-learning models. But the models themselves also need to be diligently considered. There is a great opportunity to leverage a hybrid analytics construct across unsupervised and supervised models, along with policy rules, to achieve the best results. Essentially, one can leverage self-learning (unsupervised) models to identify random anomalies in the traffic. These anomalies become features that can be leveraged to great effect in a supervised model highlighting fraud events that a rules-based approach may not notice alone. (Incidentally, an unsupervised model approach on its own, has a tendency to create a lot of false positives, as it may simply chase the anomalous traffic). So, the best practice would suggest that you marry unsupervised models, to take advantage of undiscovered anomalies, and supervised models, to leverage those insights and temper the results. If you combine this approach with a policy rules engine you can create highly targeted, accurate results.' – David Britton, VP Industry Solutions, Fraud & ID Management at Experian.[39]

The improvements in FDP technology, via machine learning, have reduced false positives and false negatives; in turn, this has improved the viability of FDP in the sector's eyes.

Fraudsters and cybercriminals are responding to the enhanced detection capabilities for transaction fraud and account fraud offered by FDP service providers. In some instances, they have also adopted machine-learning algorithms to uncover weaknesses in fraud detection systems, in an adversarial way.

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

The choice of FDP vendor is therefore critical in terms of how its machine-learning solution is implemented. FDP vendors must use a live model, which can learn and react to enhanced threats.

'Fraudsters also use automation in the form of bots, so machine-learning technology is a very powerful weapon in the fight against fraud, but it must be wielded by humans. They bring domain knowledge and recognise new threats – human vigilance is a part of the effective use of machine learning capability.' – Anand Oka, Partner Group Program Manager, Microsoft.[40]

Risk assessment alongside service provider due diligence should be viewed as key to the overall FDP procurement process.

3.3.7 The Threat of Deepfakes

Deepfake images are being used to open accounts, the use of selfie and passport capture during some KYC processes is open to deepfake abuse.

Deepfake images, videos, and voices are based on AI and deep learning. These technologies are used to manipulate video and voice data, the data is usually composed of thousands of images of two people, morphed and merged using specialist software; voice is then overlaid. The threat of synthetic identity is made more difficult to detect if deepfakes are being used to create verified identity accounts that are then tied to a payment. Some identity verification-checking companies, such as Mitek are already building anti-deep fake technology into their stack.[xlviii]

Adversarial machine learning or AI as used in offensive operations may become a tool in the war of attrition being fought by intelligent technologies. Using AI technologies to take on other AI technologies, in a gladiator-style competition, is a natural next step and is already happening, to a degree, in payment fraud. In a recent exploration of the landscape of adversarial AI 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation' researchers concluded that:

'Depending on whose bidding such systems are doing, such advanced AIs may inflict unprecedented types and scales of damage in certain domains, requiring preparedness to begin today before these more potent misuse potentials are realisable.'[xlix]

It is worth assuming that one of those domains will be financial and therefore, preparedness is warranted. As FDP becomes omnipresent across the payments' system, cybercriminals will continue to use innovative technologies to get into that system by any means. This includes creating accounts that look legitimate but are based on spoofed personal data. Highly targeted deepfake accounts may spring up; focusing on high-worth individuals. Any organisation that depends on verified identity as part of its system of payment should look to building deepfake-hardened processes.

3.4 Airlines

Airlines have been decimated by the COVID-19 pandemic. IATA's latest economic forecast reveals Europe as being the worst hit by the impact of the pandemic on the industry during 2021, with predicted airline losses of

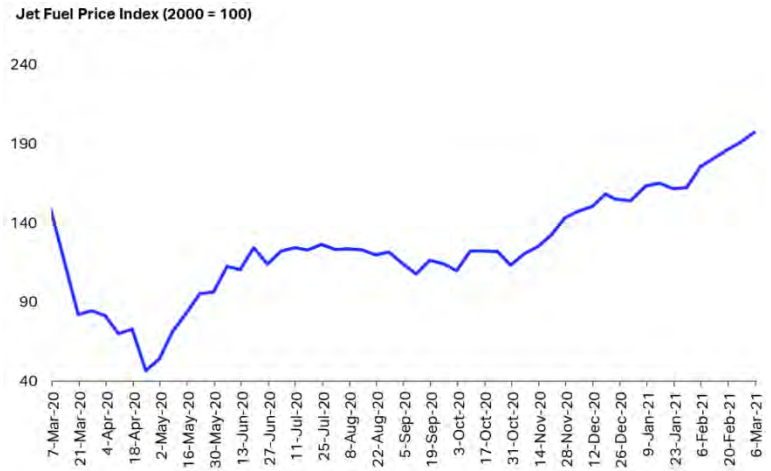
[40] Juniper Research interviewed Anand Oka, Partner Group Program Manager, Microsoft in April 2021

$11.9 billion.[i] Intra-EU bookings were down by 81% for the period to 10th January 2021. Globally, the figure for airline industry losses in 2020 is expected to be around $252 billion.[ii]

To compound losses due to grounded flights, the industry has also had to deal with fraud issues that have come about because of the pandemic, one of which is refund fraud. In May 2020, Ryanair, for example, reported that they were dealing with 10,000 times the number of refunds as usual. Flight refunds in Europe are dealt with under the EU 261 regulation that was passed in 2004. However, the sheer volume of refunds resulted in a mosaic attempt to reduce friendly fraud and chargeback fraud by substituting with vouchers or even refusing refunds on technicalities. Reputations of airlines were hit during this period.

As vaccination numbers continue to increase, and the use of travel passports to demonstrate COVID-free status are taken up, it is expected that flight volumes will begin to increase towards normality. With resumption of the industry, it is likely that the online and mobile ticket that are subject to many of the same fraud concerns, as eRetail merchants will begin to attract fraudsters again. The COVID-19 pandemic has hit the airline industry hard, and other factors including the fluctuation of fuel prices has a significant impact on airline operational costs, as can be observed in the following figure.

Figure 3.3: Jet Fuel Price between March 2020 and March 2021



Source: Platts

The gross losses and rising fuel costs during 2020/2021 mean that airlines' ability to sustain any fraud losses is at an all-time low. The impact of reducing fraud rates is a must-have for 2021 and beyond.

i. Key Challenge: Security

Despite the fact that airlines have been effectively grounded for a year, cybercriminals have still targeted the industry. In 2020, EasyJet was the victim of a cyberattack that stole the data of 9 million customers, including the credit card details of over 2,200 consumers. The attack was described as 'highly sophisticated' and the credit card detail theft may be a similar type of attack to the British Airways Magecart vulnerability attack of 2018. Some sources believe that Chinese hackers targeted a number of airlines, including EasyJet.[iii]

Airlines, even in the circumstances of the last 12 months, are still prime targets for data theft, this data then being used to perform identity theft, create synthetic identities, and any financial card data stolen used to perpetuate direct transactional fraud. Social engineering attacks, misconfiguration or app vulnerabilities, all offer ways of stealing these data.

The global customer base of many airlines inevitably means that EU citizens' data will be handled, which substantially increases their risk profile. Meanwhile, as long as cybercriminals find a reasonable level of success in targeting airlines, they should continue to be viewed as high-value targets for fraudsters. This will continue to be the case, as the airlines begin to pick up as vaccination programmes advance and holidays and business trips pick up once more.

3.4.2 Third-party Attacks

SITA, an air transport communications and information technology provider for the airline industry, was victim of a cyberattack in Q1 2021, the attack focusing on its Passenger Service System servers. SITA provides IT systems for around 90% of the global aviation. This is an example of the importance of vendor supply chain security. The British Airways Magecart attack of 2018 is another example of vulnerabilities in third-party vendor systems having a material impact on the airline industry. Third-party vendors must not be left out of the payments security equation.

3.4.3 Key Challenge: Chargebacks

A major ongoing issue for airlines has been chargebacks, which often arrive well after the original sale of the airline ticket. This elapsed time frequently results in the airline, having missed the fraud at the point of transaction, being unable to offer the seat to a genuine customer, and therefore losing out significantly. The COVID-19 pandemic saw this issue skyrocket, as refunds and chargeback attempts flooded in. In Q2 2020, IATA estimated airlines had a $35 billion refund liability in the BSP (Billing and Settlement Plan). The IATA Pay scheme that provides an Open Banking mechanism for real-time payments offered a Reverse Settlement process implemented in the industry's BSP to handle the massive amount of refunds.

In 2019, sales via the BSP totalled $237 billion, which is around 40% of total industry ticket sales of $612 billion. Overall, IATA financial settlement systems handle about 70% of indirect sales.

This issue will affect regional airlines disproportionately, which are less able to automatically screen for fraudulent online activity; leading to higher levels of fraudulently purchased tickets. Chargebacks on top of massive losses due to grounded flights may be the tipping point into bankruptcy for regional airlines. Simultaneously, they can afford to spend less time manually reviewing suspicious transactions (five minutes per transaction vs over 10 minutes for full-service carriers).[liv] That said, it should be clear that across the industry, where chargebacks are issued, the cost of the fraud goes well beyond the value of the ticket, as well as the chargeback cost.

3.4.4 Key Trends & Future Outlook in the Airline Sector

The AI-enabled payment fraud detection used in the eRetail sector is widely applicable to the airline sector, given the same challenges are generally found. Nevertheless, the continued threat of PII breaches will inevitably mean that airlines will increase their cybersecurity budgets in

the hope of mitigating these issues. At the very least, concerns about GDPR fines will encourage security best practice investment where global airlines are concerned. The British Airways breach of 2018 ended up costing the company £20 million in fines issued by the UK's ICO, and it came at a time when BA could least afford it – during the pandemic.[liii]

The airline industry is responding to the move to mobile and instant/real-time payments. IATA, using technology from ipagoo, has created IATA Pay. The payment system, which is industry backed, is offered on airline websites and utilises Open Banking and mobile/P2P payments to bank account-to-bank account direct payments.

As airlines continue to explore the omnichannel payment landscape, they must pay attention to the same issues as eRetail, including social engineering, identity theft, and CNP fraud.

Loyalty programmes are also under attack, being regarded as 'soft targets' and less noticeable. Loyalty points can act in the same way as cash; allowing purchases of gifts and stays in hotel rooms. A report from Forter described a spike in loyalty programme fraud in 2019/2020 – rising 89% year-on-year.[liv] Tactics such as credential stuffing attacks that use stolen login credentials to gain unauthorised access to accounts may be behind this spike.

The airline industry has been seriously affected by the global shutdowns preventing travel. This grounding of flights is not over yet, although vaccination programmes will hopefully change this. The industry must take fraud head-on when flights resume and take on fraud head on. Losses caused by payment fraud hurt the industry on many levels, from non-compliance fines to lost reputation to financial pain. The interwoven landscape of omnichannel payment options, coupled with strengthening of cybercriminal tactics, creates a complex landscape for airlines to manage. Revenue is drastically reduced, but fraud can tip a struggling airline over the edge. Good technology choices can help stem the flows of money out of the payment system into fraudsters' bank accounts. The use of pattern matching/AI/machine learning to spot fraudulent patterns of attack and biometrics during payment authorisation will help airlines manage this fraud. Technology usability vs acceptance vs security will be a challenge for all airlines, as it is in eRetail. New payment methods facilitated by the Open Banking API revolution may help to make the payment process seamless, secure, and instant. However, as with any eRetailer, the security of the ecosystem behind this payment method must be robust.

4. Online Payment Fraud: Competitor Analysis

4.1 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

4.2 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 4.1: FDP Vendor Capability Assessment Criteria

Category	Criteria	Weighting	Description
Capability & Capacity	Financial Performance in Sector	20%	In assessing this factor, we considered the vendor's FDP performance as measured by revenue, number of employees and investments.
	Experience in Sector	30%	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	10%	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	25%	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, eg in-country sales specialists and VARs (Value-added Retailers).
	R&D Spend	15%	An indicator of the investment a vendor is making to develop best-in-class solutions; M&As are considered here as a measure of investment.
Product & Positioning	FDP Product Range & Features	30%	This factor relates to breadth of product range coverage by platform, technology and channels.
	Customers & Deployments	10%	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	30%	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	20%	This factor assesses the vendor's perceived innovation through its flow of new features, products, developments and improvements.
	Future Business Prospects	10%	This factor relates to the business' ability to develop and compete against others in the future.

Source: Juniper Research

4.3 Leaderboard Scoring Results

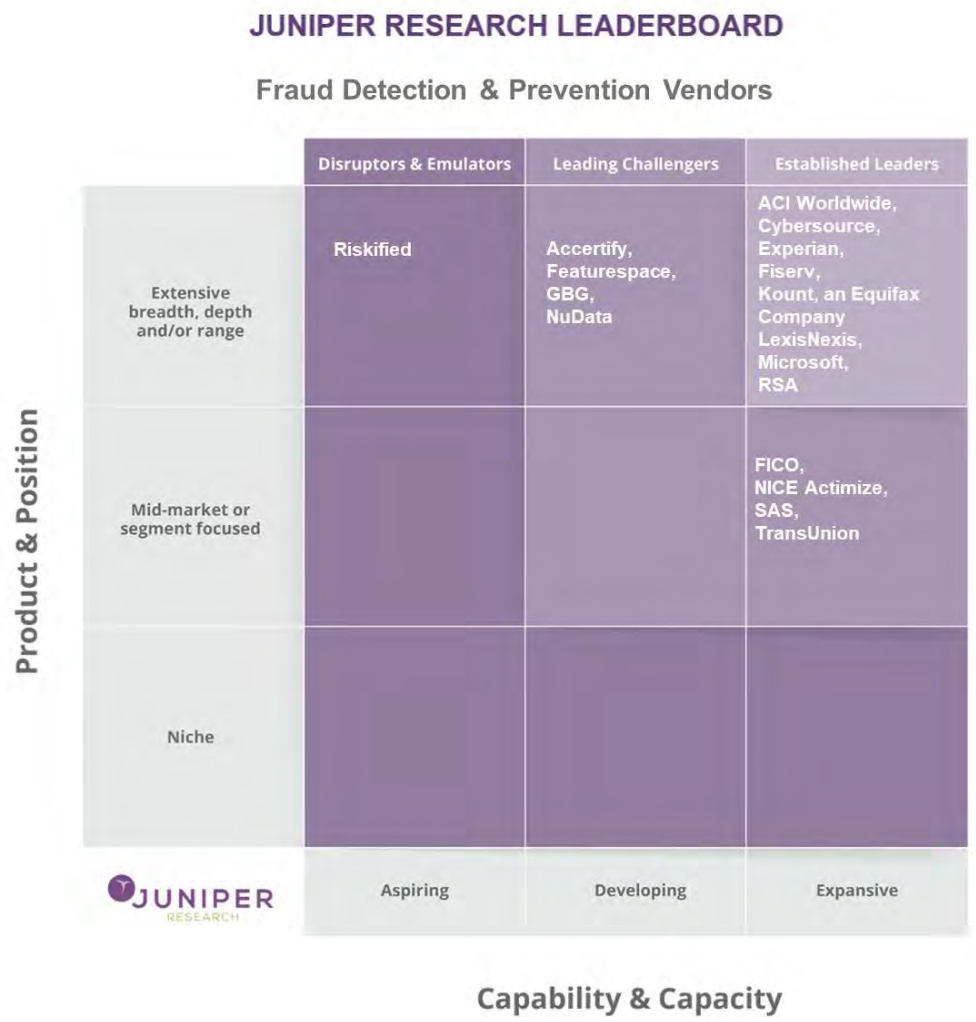
Table 4.2: Juniper Research Leaderboard: FDP Vendors

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

HIGH LOW

Source: Juniper Research

Figure 4.3: Juniper Research Leaderboard: FDP Vendors



Source: Juniper Research

4.3.1 Stakeholder Groupings

Our analysis enables us to conclude that, from this particular list of vendors, there are essentially three main groups.

- Established Leaders
- Leading Challengers
- Disruptors & Emulators

Many key acquisitions across the space have moved a number of previously leading challengers into the established leaders space.

i. Established Leaders

- ACI Worldwide has developed a very valuable fraud prevention solution that has experience in, and the ability to cater to, the unique needs of many different global markets. Its offering of the ACI Proactive Risk Manager incorporates machine learning and predictive analytics, meaning that this is an extremely high-value solution. Key partnerships keep the larger vendor agile.
- Cybersource offers a single platform at significant scale, which is boosted by its integration with Visa's widespread payment network. Again, machine learning is a central pillar of Cybersource's offering; adding significant value and improving detection rates. The new partnership with Planet will open up new revenue opportunities.
- Experian continues to invest into its FDP solution and use the companies vast array of customer data to deliver an effective machine learning module that takes into account multiple dynamic sources of data. This, in combination with the CrossCore platform's wide range of abilities, including the ability to integrate solutions from third-party vendors and its integration with Hunter, make it highly valuable.
- Fiserv's Financial Crime Risk Management Platform is a comprehensive and effective solution for fraud prevention and management for banks and FIs. Strong strategic acquisitions in 2020/2021 allow Fiserv to diversify and strengthen its core capabilities.
- Kount, an Equifax Company has emerged as an AI-powered competitor in this space, by harnessing data and intelligence from 8,000 digital businesses and payment providers. Kount has high potential in the space, strengthened by the acquisition of the company in 2021 by Equifax.
- LexisNexis has built on a strong position in the credit and identity space by acquiring ThreatMetrix; bringing it under the Risk Solutions area. Strong strategic acquisitions in 2020/2021 allow LexisNexis to add to its core capabilities.
- Microsoft has built an FDP service based on machine learning. The company is able to draw upon its vast network of vendors to understand the features and capabilities needed by retailers. Microsoft, as an established international company, will be able to make headway into other sectors as and when they decide to do so.
- RSA Security has developed critical expertise in both fraud prevention and cybersecurity; this will become more valuable as customers recognise the relationship between the two.

ii. Leading Challengers

- FICO has a long track record of providing valuable, data-driven, risk-based approaches, which has led to the production of a leading FDP solution. FICO's solution is advanced, as it uses a combination of AI and human intelligence to provide a holistic approach to managing payment security. They have recently expanded their capability through a strategic partnership with Open Banking vendor OpenWrks.
- SAS offers a comprehensive solution that is able to detect and manage fraud holistically, which will continue to be essential, given the evolving nature of the fraud landscape. The company is also heavily involved in keeping track of new fraud methods, so can be expected to provide ongoing leadership in preventing innovative fraud.
- Accertify is a leader as it is able to offer customers an all-in-one solution of payment gateway, alongside fraud prevention and management, which is bolstered by its integration with American Express' network. The addition of ID support now gives Accertify a truly cross-lifecycle, anti-fraud view.
- Featurespace is a force within the industry and continues to push both commercially and in terms of innovation in FDP capabilities.
- GBG PLC has consolidated its efforts around FDP by utilising its already strong presence in the ID space and acquiring strategic vendors. This positioning will position it well against competitors that have less experience in the fraud space.
- NICE Actimize continues to iterate on a robust FDP solution, which is geared to the financial industry. Further acquisitions strengthen the company in the small- to medium-enterprise sector.
- NuData has developed advanced capabilities in positive identity confirmation through machine learning and biometric analysis. The changing nature of fraud means that there is significant potential here and it will be able to harness significant benefits from access to Mastercard's network.
- TransUnion, through the acquisition of iovation, continues to be one of the leading vendors in terms of user or device authentication, and this is supported by its comprehensive device ID database. The access to vast amounts of user data provides the basis for cutting-edge FDP technology.

iii. Disruptors & Emulators

- Riskified has emerged as a strong disruptor in the FDP space, but is very focused on the specific eCommerce area. It has momentum, and new investment, which it will likely use to expand its offerings in terms of scope.

4.3.2 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.

4.4 Vendor Profiles

4.4.1 Accertify

Juniper Research interviewed an Accertify representative in April 2021

i. Corporate

Established in 2007, Accertify is a provider of fraud prevention, chargeback management and payment gateway solutions to merchants for a range of verticals worldwide. It is a wholly owned subsidiary of American Express and is based in Illinois, US. Some 400 individuals work for the company, in seven countries.

Accertify has been successful in selling its fraud detection and management solution in the eCommerce space to over 200 enterprise customers, including major airlines, retailers, ticketing and entertainment, financial services, payment processors and social networks.

Key executives at American Express include Mark Michelon (President); Randy Ruiz (CTO); Catherine Malec, (VP & General Manager, EMEA).

In July 2020, Accertify launched ADI (Accertify Digital Identity), a solution to help organisations address the rise in fraudulent online account openings and account takeovers. The product is an API-based solution that empowers organisations to trust and verify who is on the other side of a digital interaction. The product was awarded best identity/authentication solution at the 2021 Merchant Payment's Ecosystem conference.

ii. Geographic Spread

Accertify offices serve a global customer base and are in the US, the UK, Mexico, India, Japan and Australia.

iii. Key Clients & Strategic Partnerships

- Accertify highlighted key partners in a recent interview: 'Accertify has key partnerships with Mastercard, Worldpay, TSYS, Amadeus, everis, Ekata, and Emailage.'
- Accertify has been particularly successful in attracting numerous airline customers, including JetBlue, Southwest Airlines and Ryanair, EasyJet and British Airways. Other high-profile clients include Urban Outfitters, Marks & Spencer and Greyhound.
- Alongside six of the top ten global airlines by revenue, Accertify has 20 of the top 50 US eCommerce retailers as clients, as well as a customer base comprised of financial service providers, ticketing and digital goods merchants.
- The company reports that 39% of its clients have their headquarters outside the US.

iv. High-level View of Products

The size (in terms of transactions and events) of the data that Accertify is able to leverage from its widespread customer community database is substantial. In turn, this is a key element behind the success of its machine-learning capabilities.

Accertify's platform enables merchants to screen for multiple fraud cases including, but not limited to payment fraud, loyalty, claims, staff and social

media reputation. The company's unique capabilities allow genuine customers to be efficiently removed from fraud processes; supporting merchant growth.

The Accertify Interceptas® Platform is a 'Software-as-a-Service' offering that allows clients to customise and adapt their fraud-screening strategy in real-time; leveraging best-in-class industry machine-learning models, configurable fraud and policy rules, and robust reputational community data.

- Scoring Functionality: At its core, the Interceptas® Platform is a data management tool. By offering a rich set of integrated machine-learning models, pre-built rules and condition checks, clients can implement a near-infinite range of policy checks to live alongside their fraud-screening strategy.
- Case Management: The Interceptas® Platform offers clients an incredibly configurable tool for analysing, risk assessing, reporting on and managing fraud risk screening.
- Machine Learning: Powered by Dynamic Risk Vectors, Accertify's machine-learning capabilities power the creation of new predictive data elements for use in industry models.
- Device Intelligence: Accertify Device Intelligence analyses devices and associated identities transacting across digital channels via mobile applications (InMobile) and mobile and desktop browsers (InBrowser).

InMobile provides a SDK (Software Development Kit) that can be incorporated into mobile applications to access detailed mobile device information.

- User Behaviour Analytics: Accertify offers their clients the ability to easily identify human vs bot traffic by analysing user behaviour and quickly alerting for bot detection.
- Link Search Capabilities: Accertify's enhanced link search functionality gives clients the ability to search for historic linkages that can clarify whether an event is out of pattern, or in fact is evidence of a loyal, repeat customer.
- Rules/Conditions Testing: Clients can test and simulate a condition or conditions using the Accertify rule testing 'Sandbox.'
- Profile Builder: Profile Builder helps identify real-time patterns and trends through the dynamic summarisation and aggregation of data.

Accertify's Chargeback Management Solution: Reduces the resources required to manage and respond to chargebacks by up to 50 percent.[lv] It offers a 'Software-as-a-Service' platform that clients can manage themselves or they can outsource the end-to-end management of chargebacks.

Payment Gateway: This complementary product is for clients seeking a singular platform for payments and fraud.

Services offered include:

- Decision Sciences: Accertify's global team of machine-learning experts and data scientists focuses on three core areas; building industry-leading machine-learning models; client consultation; research and development.

- CSM (Client Success Management): Accertify's global team of Client Success Managers is responsible for ensuring each client is achieving their fraud and chargeback goals and are aware of new features and functionalities.
- Managed Services: Provides direct operational management of the fraud and/or chargeback processes leveraging the company's industry-leading Interceptas platform.
- Professional Services: Accertify offers a wide range of professional services designed to help clients optimise fraud prevention, chargeback management, and payments performance.
- Support Services: The global Support team delivers white glove, world-class 24/7 service, every time for every client.

Accertify SCA Optimisation was designed to support clients' compliance efforts with the SCA directive and, at the same time, reduce unnecessary friction to the consumer journey during the check-out process by managing SCA exemption and scope checks.

SCA Optimisation combines Accertify's logic-based rules capabilities with its machine learning fraud screening solution to risk score transactions and then assess them for SCA purposes. The transactions are risk assessed prior to authentication. Those which pass the risk-scoring are then assessed from an SCA perspective. Identifying riskier payments prior to competing the SCA assessment helps reduce the number of transactions which are submitted for an exemption. Removing these transactions at the pre-authentication stage ensures that the merchant maintains a good fraud profile with issuers, thereby helping ensure high approval rates on future authorisation and exemption requests.

The SCA assessment informs the merchant whether the payment is out-of-scope, in-scope but can be exempted or, is in-scope and cannot be exempted. Identifying payments that are either out-of-scope or can be exempted enables the merchant to avoid unnecessary friction being added to the customer checkout experience.

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- Accertify's size (in terms of transactions and events) and ability to take advantage of marquis customer community database, means that it has a vast array of data available to enhance its machine learning capabilities. This will help to train algorithms in new vectors and threats; keeping Accertify at the forefront of fraud detection.
- Accertify cover a wide range of fraud types. This gives the company a way to continually push into new markets as the fraud landscape changes.
- Behavioural analytics and the mobile SDK is an important capability when determining if a transaction is bot or human. As more credential stuffing attacks occur, after mega breaches, this will be a useful part of the Accertify platform.

4.4.2 ACI Worldwide

Juniper Research Interviewed Benny Tadele, VP, Merchant Payment Solutions, and Amanda Mickleburgh, Product Director Merchant Fraud, ACI Worldwide in March 2021

i. Corporate

ACI Worldwide is an international provider of global payment and banking systems. Founded in the US in 1975, it is a publicly listed company and trades on the NASDAQ (ACIW).

Key executives at the company include Odilon Almeida (President and CEO); Mike Braatz (Chief Strategy Officer); Eve Aretakis (Chief Revenue Officer); Scott Behrens (CFO). The company employs around 4,000 people.

Figure 4.4: ACI Worldwide Financial Snapshot ($m), 2017-2019

	2017	2018	2019
Revenue	$1,024.2	$1,009.8	$1,258.3
Net Income	$5.1	$68,921	$67,062

Source: ACI Worldwide

- ACI Worldwide is a global software company that provides mission-critical, real-time payment solutions to corporations. Customers use our proven, scalable and secure solutions to process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk. It combines its global footprint with local presence to drive the real-time digital transformation of payments and commerce.
- 2020 results look-up on 2019:
  - Revenue of $1.294 billion, up 3% from 2019
  - Net income of $73 million, up 8% from 2019

ii. Geographic Spread

ACI's headquarters are in Florida, US. The company has offices in 34 countries across the US, Asia, Europe, South America, Africa and Australasia.

iii. Key Clients & Partnerships

- ACI has numerous partnerships in place across the payments landscape, with key brands including Accuity, Barclaycard, Citrus Pay, Discover, Experian, Fiserv, Gemalto/Thales, iovation, Sagepay, Evo Payments, Mastercard, PayPal, RSA, ThreatMetrix and VeriFone, among others.
- Customers include Wendy's, HSBC, Dominos Pizza, Wells Fargo, and Mastercard. No single client brings in more than 3% of revenue.
- Meanwhile, technology partnerships have been established with companies such as HP, IBM, Microsoft, Red Hat (which was acquired by IBM in 2018) and Oracle.

- Stet, with over 300 banks in France and Belgium, partners with ACI to provide instant payment adoption using a one-stop-shop approach.
- Mastercard and ACI partnered in 2021 to modernise Peru's real-time payments infrastructure. ACI is helping financial institutions in Peru manage the transition to the new ISO 20022 standard by offering an adaptor solution based on the ACI Enterprise Payments Platform.
- ACI extended its partnership with Boots the Chemist (part of Walgreen's) to utilise ACI Omni-Commerce, a secure, validated P2PE omnichannel payments platform, which will help meet the requirements of SCA.
- 'ACI works with partners to drive accuracy in detection capabilities, using age, device ID, citizen verified ID, eg in Brazil, CPF validation, etc.' – Amanda Mickleburgh, Product Director Merchant Fraud, ACI Worldwide

iv. High-level View of Products

ACI has a comprehensive suite of payments solutions, for retail and corporate banks, merchants, billers, and payment intermediaries, including PSPs, processors and acquirers. ACI's solutions help customers process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk.

ACI offers payments and fraud management solutions with machine learning, including a global eCommerce payments gateway and a fully integrated eCommerce fraud prevention solution. The company places an emphasis on real-time payments. eCommerce solutions are complemented by in-store payments and payment security capabilities to deliver a full omnichannel payments capability that is underpinned by a single omni-token. The platform offers rich APIs that allow the creation of tailored customer journeys, while enabling fast and PCI-descoping integration mechanism.

'Transaction comes in and the data is pushed through a RESTful API gateway – allowing a wide range of data points to be sent in by a customer. This is then pushed through multiple layers of technology, including our global consortium database (positive/negative profiling) – to query it against ACI's global view.' – Amanda Mickleburgh, Product Director Merchant Fraud, ACI Worldwide

ACI Omni-Commerce and ACI Secure eCommerce solutions are available globally and focus on Tier 1 and Tier 2 merchants around the globe, along with payments intermediaries including PSPs, Merchant Service Providers, Independent Sales Organisations and VARs.

The solutions are aimed not only at fraud prevention, but also at improving merchant profitability by virtue of increasing the accuracy of positive identification of genuine customers. This is achieved via ACI's stream analytics engine, which uses up to 100 features to identify customers, as well as information retrieved from the ACI consortium database, which collects data globally from thousands of merchants. In this manner, identification of the customer becomes key to both fraud prevention and reduction in additional friction at the checkout.

Amanda Mickleburgh told Juniper Research:

'ACI has focused on machine learning and files patent in the area to continuously improve their product capabilities. ACI's models not only

predict fraud, but also learn and mould themselves to new behaviours, ensuring customers are always protected from fraud, even when fraudulent activity changes and becomes more sophisticated than before.'

For its fraud management solutions, ACI offers two types of business models:

- SaaS- and PaaS (Platform as a Service)-based Hosting: The company's solutions are delivered as part of a cloud-hosted single tenant (SaaS) or multi-tenant (PaaS) environment, dependent on the volume of transactions processed and the number of solutions purchased by the customer. Data centres are located across the globe to support this model.
- Licensed/on-premises: Customers deploy ACI software over their own infrastructure under a licensing term that typically lasts for 60 months.

There are a small number of ACI's FI customers that outsource the solution to ACI at the company's hosting facilities. However, they still manage the rules, behaviour profiling and set up the alerts as they want. ACI does this for customers from the consumer banking side, as well as the transaction banking side or commercial side.

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- ACI is has a strong global reach and uses market intelligence to ensure their products stay ahead of market needs. This is reflected in its in-house innovation, as well as in purchases such as Speedpay.
- The company's other offerings as a payments gateway mean that it more intimately understands payments challenges than other vendors, meaning that it can offer highly effective products.
- eCommerce and consumer fraud are ACI's domain expertise areas. ACI solves complicated issues for merchants, such as ensuring that transactions are verified across the entire ecosystem. ACI offers seamless merchant use of this capability through their SaaS platform. In doing so they act as the glue that helps de-risk the payments ecosystem.
- ACI must keep pace with large competitors who are buying up more agile vendors in the space.

4.4.3 Cybersource, a Visa Solution

Juniper Research interviewed Andrew Naumann, VP Product Management, Cybersource in March 2021

i. Corporate

Cybersource is a wholly owned subsidiary of Visa, Inc. Established in 1994, Cybersource helped kick start the eCommerce revolution in 1994. In 2007, Cybersource acquired Authorize.net to cater to small businesses, and in 2010, Cybersource was acquired by Visa Inc for $2 billion. Visa has approximately 20,000 employees in global offices and data centres around

the world. Headquartered in San Francisco, California, Cybersource serves more than 468,000 businesses worldwide. Cybersource is a global, acquirer-agnostic modular payment orchestration platform. At the heart of Cybersource is a modular, cloud-based platform on a network with uptime at 99.999%. Using a single set of APIs, Cybersource can integrate with any system in the market and support any vertical: Retail, eCommerce, transit, telcos, restaurants, airlines, insurance and utilities. The modular platform enables clients to:

- Reach further: Cybersource's global scale enables payments in over 190 countries, and support over one million users.
- Adapt faster: Cybersource's modular services give merchants the flexibility to design a tailored experience for their customers, with payments seamlessly embedded.
- Grow stronger: Cybersource was a key player in the eCommerce revolution in 1994 and has been at the forefront ever since. Today, it helps over 468,000 businesses to grow and stay protected from fraud.

Cybersource enables unified commerce, accessed and managed via a single platform, across all channels, via flexible APIs. Helping businesses maintain maximum agility in their payment operations, and execute omnichannel experiences securely and seamlessly on a global scale.

Cybersource is led by general manager, Carleigh Jacques, with product management led by Andre Machicao.

Figure 4.5: Visa Financial Snapshot ($m), 2018-2020

	2018	2019	2020
Revenue	$20,609	$22,977	$21,846
Net Income	$10,301	$12,080	$10,866

Please note financials are for Visa only and do not represent specific Cybersource financials.

Source: Visa

ii. Geographic Spread

Cybersource's payment management solutions are available in over 190 countries and territories.

iii. Key Clients & Strategic Partnerships

Cybersource partnered with Planet in 2021 to launch a new digital payments platform for European merchants. The new service delivers solutions to merchants across hospitality, food and beverage, and retail sectors to simplify complex digital payments.

In 2020, Cybersource and Nuapay formed a strategic integration between Cybersource Payment Gateway and Nuapay's end-to-end cloud platform for recurring payment collection; covering payer sign-up through to managing money received.

Cybersource is tightly integrated into sister company, Cardinal Commerce, also a Visa solution; helping retailers with consumer authentication integration.

Cybersource offers compelling payment and fraud solutions with several key technology partners; SAP, Salesforce Commerce Cloud, Sitecore and Zuora are all pre-integrated technology partners.

Evolving towards a one-to-many relationship with resellers to promote and sell products.

iv. High-level View of Products

Visa's 2020 Annual Report specifically pulled Cybersource out as an example of value-added service revenue-generating part of Visa. Saying that 'acquirers and merchants actively sought Cybersource's offering as they looked for ways to evolve their business models and meet shifting consumer behaviours accelerated by COVID-19.'

Cybersource's platform encompasses a complete portfolio of online and in-person services that simplify and automate payment operations. Cybersource is the complete solution for eCommerce merchants. The solution has a depth and breadth, that includes, payment processing, digital commerce solutions, and fraud and risk management. Cybersource enables merchants to access those services from a single integration but how these services interrelate is important, so the approach is holistic.

'In 'Masters of Balance: What it takes to be a fraud management leader,' Cybersource's 2019 Global eCommerce Fraud Management Report, many businesses reported they brought their fraud losses largely under control and stabilised them at levels that minimise negative impacts to revenue or customer satisfaction.' – Cybersource Revenue Capture whitepaper 2020

DM (Decision Manager) is Cybersource's flagship enterprise-level risk management solution that helps manage fraud and increase customer satisfaction. Decision Manager allows businesses to make risk adjustments to stop fraud before it starts, and it helps detect more good orders quickly. This delivers greater insight for businesses and adds value to every transaction. It combines 16 region-specific, channel-specific, and industry-specific machine-learning risk models that use the consortium of data from the entire Decision Manager merchant base to optimise accuracy with various detection tests, a fully customisable rules engine, case management capabilities, and real-time reporting.

DM's key features include:

- Multiple, proprietary machine learning algorithms, which automatically assess the risk of each transaction; drawing on data insights from the more than 141 billion worldwide transactions processed annually by Visa and Cybersource. These out-of-box predictive risk models are configurable.
- Flexible Rules Engine, which contains pre-loaded standard rules and customisable rules that are collectively applied for each transaction or event.
- An integrated case management solution to manage and prioritise transactions selected for manual review. Case management includes a review dashboard, configurable review queues and service-level agreement management to support enterprise-level fraud teams.
- Decision Manager Replay is the industry's first fraud tuning analytics tool, that enables merchants to quickly test new fraud strategies against their historic transaction data; resulting in a side-by-side display of results before deciding if new strategies should be put into production.

Merchants create rules and parameters in their fraud management systems to determine whether to accept or deny a transaction, based on risk level. In some cases, the parameters they set might be overly cautious; causing them to lose legitimate, safe business unnecessarily. This offering allows merchants to backtest prior transactions to see what would have happened if they had set different rules.

Decision Manager offers a number of use case options where different attributes and data elements are used as appropriate. These include account takeover, rules-based authentication, fraud alert, loyalty fraud, etc.

The company also provides a unique service dubbed Rules Suggestion Engine. Machine learning algorithms are applied to historical data, which then suggest new fraud prevention rules or amendments to existing rules. Each suggested rule is accompanied by appropriate metrics to help measure its performance against selected transaction data.

For those enterprise businesses which need complementary fraud expertise, Cybersource offers Managed Risk Services. This allows global risk analysts to help merchants design, implement and maintain a fraud management platform that is customised for their business.

Cybersource's fraud risk analysts can provide support 24/7 in five continents.

In addition to pure fraud prevention tools, the company also develops payment security services which ultimately help reduce payment and account fraud:

Cybersource has developed innovative payment solutions for today, and a flexible and scalable foundation for the future. With the acquisition, and full integration of Payworks, it can offer an omnichannel payment management platform that can flex, as the commerce experience continues to evolve through multiple channels and multiple payment methods.

- Secure Acceptance enables merchants to take digital payments without having to handle any payment data. This service is supplied in the form of a checkout page, which includes built-in support for Decision Manager. Additionally, the solution offers a checkout token service which integrates with merchants' own checkout software.
- TMS (Token Management Service) is a payment tokenisation service that mitigates payment security risk for businesses by securely vaulting sensitive payment data in Visa data centres. TMS standardises token management across payment types, channels and providers; enables omnichannel experiences; powers customer analytics and marketing programmes; increases operational agility.

  Cybersource develops all its technology in-house, although it relies on a small number of leading datapoint providers. It offers a SaaS-based hosted service only.

'As eCommerce goes mainstream, we needed to find a solution where a smaller retailer could get an FDP up and running really quickly. We can minimise fraud costs and reduce chargebacks for the smaller retailers. We are building the building blocks for the entire customers journey.' – Andrew Naumann, Product Management, Cybersource (Visa)

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- Cybersource's access to the Visa's network for risk modelling and data sourcing places it in an enviable position in the sector. Using this data source allows Cybersource to utilise 140 billion transaction per year worth $214 billion. This means that Cybersource has a massive ability to train its machine learning to be much more effective. This link to a major FI also adds weight to the company in developing important strategic relationships to add value to its gateway and vice versa.
- Cybersource has a key strategic pathway in partnering with core offerings in the retail and merchant marketplace. This will ensure the company has many avenues for continued growth and push into both existing and new sectors.
- The ability to offer a payment gateway alongside fraud prevention allows Cybersource to be viewed as a 'one-stop' solution by many merchants, which is compelling given that other vendors in the area cannot offer this. Given that Visa has been acquiring many vendors recently, this offers Cybersource future partnership opportunities.
- Cybersource plans to upgrade Decision Manager; keeping abreast with increasingly complex variables across payments. The next upgrade of Decision Manager will support API-based smart routing and will have the ability to configure rules on any API field in order to have the transaction routed appropriately. Also, DM will route transactions based on aggregated parameters (dollar amount, volume, etc).

4.4.4 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 (now part of the new Decisioning 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 4.6: 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 on 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, eg 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, but include all contracting and due diligence with the vendor, so that the client only needs to amend their MSA 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

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- Experian continues to strengthen its brand through consumer focus. The company has secured direct relationships with 82 million consumers (up from over 55 million in FY19 and have 29.5 million free members in the USA, 45 million in Brazil and 7.5m in the UK).

- CrossCore's USP is in its orchestration platform with a single API input. This provides a powerful engine, augmented by data input from partner organisations. This connectivity across many data sources is a key differentiator. The orchestration of these data with machine learning-enabled analysis has created a highly advanced solution.

- Experian is in a unique position because it sits in both the identity verification and fraud management camps. As these two areas more closely align and even merge, Experian can use its deep know-how in both spaces to deliver more appropriate and effective products. Juniper Research expects that Experian will use its data expertise to verify identity, as well as payment transactions using a ID Network approach.

4.4.5 Featurespace

FEATURE SPACE

i. Corporate

Founded in 2008, Featurespace is a behavioural analytics company. The company was formed when Betfair asked Featurespace to build the first system to outwit fraud attacks by thinking like each one of their customers.

In 2020, Featurespace raised £30 million (USD 37.4 million) to support continued growth. In total, Featurespace has raised around $108 million in seven rounds.

Key executives include Martina King (CEO); David Excell (Founder); Simon Rodgers (CTO).

ii. Geographic Spread

The company's UK headquarters are in Cambridge, but Featurespace also has an APAC headquarter in Singapore and office in the US and London.

iii. Key Clients & Strategic Partnerships

- Featurespace signed a contract with NatWest in 2019 for an enterprise-wide deployment of ARIC Risk Hub to detect anomalies and protect customers in real time by collating account-level data across all touch points.
- CSI partners with Featurespace to integrate with Featurespace's Adaptive Behavioral Analytics platform to provide the engine behind WatchDOG AML solution.
- Australian fintech, Hay, uses Featurespace's ARIC Risk Hub to detect and prevent fraud and money laundering on its mobile-first solution.
- Featurespace creates an annual Financial Crime report that features market experts' views. The report points out that it expects the new US-based eCBSV (Consent Based Social Security Number Verification) system to be an important way to mitigate synthetic ID fraud.[lvi] The report also highlights the use on machine learning in AML and expects it to become mandatory.

iv. High-level View of Products

The ARIC Risk Hub is Featurespace's flagship products. It processes 50.4 billion events per year and provides a 75% reduction in false positives. The mantra of the company is to allow technology and human operators to work in symbiosis. ARIC is a real-time decisioning platform that has been shown to block 75% of fraud attacks. The ARIC Risk Hub has applications across industry sectors, but Featurespace puts emphasis on gaming, merchant onboarding, and banking application fraud. The solution is designed for payment and card fraud, as well as AML checks.

- ARIC Risk Hub: Featurespace's flagship product is the Adaptive Behavioral Analytics system, ARIC Risk Hub. The hub adaptive machine-learning models to protect against financial crime. The hub uses two Featurespace systems; ABA (Adaptive Behavioral Analytics) technology and unique AMDL (ARIC Model Definition Language). Individual behavioural activity is monitored in real-time and the alert

system is based on rules to allow prioritisation to help in building a cohesive relationship between the technology and human operators. This enables suspicious activity detection with greater accuracy, whilst reducing the number of genuine transactions declined.

- In 2021, Featurespace released their Automated Deep Behavioral Networks based on deep learning technology aimed at the card and payments industry. This is now integrated into the latest version of the ARIC Risk Hub. This system delivers a deep layer of defence to protect consumers from scams, account takeover, card and payments fraud.

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- Featurespace is a highly innovative company building deep learning capabilites into their core platform. The company's focus on Adaptive Behavioral Analytics is an excellent mechanism for balancing fraud checks against good customer experience.
- Juniper Research expects Featurespace to go from strength to strength as they build networks in the industry. They are likely to become an attractive acquisition by one of the larger vendors for their innovative ARIC Risk Hub.

4.4.6 FICO

FICO

i. Corporate

Founded in 1956 as Fair Issac & Company, FICO is based in California, US, and is traded on the New York Stock Exchange. FICO has around 3,668 worldwide employees. FICO is a predictive analytics and decision management software company that makes use of Big Data to predict consumer behaviour.

FICO is known in the US for its FICO Score product, which has become the standard for measuring consumer credit risk in the US. However, FICO is also active in the FDP market through its Falcon fraud platform.

An antitrust investigation into potential exclusionary conduct by FICO was launched in 2020, prompted by competitors in the space. The case is ongoing but FICO is confident that this the case will be discredited.[lvii]

Key executives include William Lansing (CEO); Wayne Huyard (EVP, Sales, Services and Marketing); Claus Moldt (EVP, Chief Product and Technology Officer).

Figure 4.7: FICO Financial Snapshot ($m) 2018-2020

	2018	2019	2020
Revenue	$1,000.1	$1,160.1	$1,294,562
Net Income	$126.5	$192.1	$236.4

Source: FICO

ii. Geographic Spread

Apart from its Californian headquarters, FICO operates from 25 locations across the globe, with offices in North and South America, Europe, Africa, Asia and Australasia. They have customers in 120 countries.

iii. Key Clients & Strategic Partnerships

- FICO has partnered with Linktera, a Middle East vendor specialising in AI-powered risk management. Linktera sells and implements FICO's decision management solutions that help banks and other credit grantors manage risk and expand lending growth.
- FICO is utilising Open Banking capability by partnering with UK-based OpenWrks to improve affordability assessments for existing customer management and collections activities. The two companies will combine Open Banking data with conversational AI to provide self-service by completing an affordability assessment digitally and remotely, dramatically reducing operational costs and improving customer experience. FICO and OpenWrks will develop and deploy a new suite of analytics to unlock the value in Open Banking data to improve consumer and business lending decisions.
- The company has a partnership with Mastercard. Every transaction that goes through the Mastercard Network is sent to FICO, which uses this data in its Fraud Predictor solution. As this product is built with Mastercard data, FICO has a revenue share agreement with the company.
- FICO's clients include more than half of the top 100 banks in the world, more than 600 personal and commercial line insurers in North America and Europe including the top 10 US personal lines insurers, over 400 retailers and general merchandisers, including one-third of the top 100 US retailers, 95 of the 100 largest FIs in the US and all the 100 largest US credit card issuers.

iv. High-level View of Products

Fico has three sections:

- Applications: On-premises or SaaS
- Scoring: Consumer credit scoring
- Decision management: FICO Decision Management Suite

FICO's main fraud product is the Falcon Fraud Manager platform, a real-time transaction event monitoring and resolution platform that allows institutions to implement fraud protection with an end-to-end holistic approach.

First introduced in 1992, Falcon is used by 9,000 FIs worldwide. It is one of the financial industry's leading fraud solutions, based on the number of FI customers.

Fraud data is augmented by the company's Falcon Intelligence Network, which is a consortium approach to data collection and analysis. This is an ongoing contribution of transaction and tagged fraud data from over 9,000 global institutions that participate in the FICO Falcon Intelligence Network. This allows FICO to continuously innovate new machine-learning approaches to predict, prevent, and stop emerging types of fraud.

In this context, anonymised behavioural and transaction-related data is processed by the company's data scientists and used as part of its supervised machine-learning initiative to help future iterations of the Falcon Platform detect fraud. The company reports that this has helped both reduce CNP fraud and the number of false positives per transaction.

In addition to pure transaction fraud analytics, the platform is able to interpret behaviour for a number of channels and services, and provide risk scoring for authentication platforms, as well as P2P transfer services and instant payment schemes.

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- FICO's ability to call upon massive amounts of financial data across its extended intelligence network means that it can keep up to date with changing global profiles as new threats emerge.
- A strength for FICO is the use of machine learning on its platforms, which has massive benefits in combatting new types of fraud.
- The company is in a highly competitive space and innovation is a must to ensure continued success in the area.

4.4.7 Fiserv

fiserv.

i. Corporate

Fiserv was founded in 1984 after the merger of Sunshine State Systems and First Data Processing. Fiserv went public in 1986, when it was valued at $70 million.

Fiserv has a strong history of acquisitions, the latest being that of First Data for $22 billion in 2019. Fiserv shareholders now own 57.5% of the new company, while First Data shareholders own 42.5%. The merger was completed at the end of July 2019.

First Data itself has made some significant acquisitions since its inception in 1969. In 2020, Fiserv made three acquisitions:

- Merchant Pro Express: A credit card processing system to consolidate Fiserv's payment solutions, CoPilot, CardPointe and Clover, with the onboarding services of MerchantPro Express.
- Bypass Mobile: POS vendor, systems of which were already deeply integrated into Fiserv's.
- Ondot Systems: Ondot was acquired to expands Fiserv digital capabilities, to enable clients to deliver frictionless, digital, consumer experiences.

Figure 4.8: Fiserv Financial Snapshot ($bn), 2019-2020

	2019	2020
Total Revenue	$10,187	$14,852
Net Income	$975	$914

Financial Year End 31 December Source: Fiserv

First Data and Fiserv merged under the umbrella of Fiserv in 2019, the benefits of the merger include:

- Savings estimated at $500 million over a five-year period.
- About $900 million in run-rate cost synergy savings (eg streamlined technology infrastructure, increased operational efficiencies, among others) are also forecast over the next five years. These savings are expected to make combined earnings rise by 20% in the first year.

- Increased cashflow in excess of $4 billion in the three years following the merger.

The combined company – Fiserv – currently has around 44,000 employees. The company serves thousands of FIs and millions of businesses across 100 countries. Fiserv is a NASDAQ 100, FORTUNE 500, Forbes Global 2000 and the S&P 500 company.

Frank Bisignano is president and CEO. Fiserv has ten board members.

In February 2021, Fiserv was named one of FORTUNE Magazine World's Most Admired Companies for the eighth consecutive year.

ii. Geographic Spread

Fiserv headquarters are in Brookfield, WI. Fiserv has offices in over 100 countries, including in the EMEA, Latin America and Asia Pacific.

Fiserv stresses that both geographic footprint and local presence are important to stay competitive in the market. The company's global footprint is broad, but also mixed with local resources and knowledgeable people who understand the market. This enables Fiserv to serve all segments of the market, from cross-border multinational commerce to local companies.

iii. Key Clients & Strategic Partnerships

- Fiserv has a strong foothold in the fintech services technology sector; offering its services to thousands of businesses worldwide, especially mega banks, thrifts, credit unions, investment management firms, leasing and finance companies, retailers, merchants and government agencies. Notable clients include Bank Liberty, Central Bank, Staley Credit Union and Santander, among others. Fiserv secured several partnerships including:

- In January 2021, the company completed its previously announced acquisition of Ondot Systems, Inc, a digital experience platform provider for financial institutions.

- In March 2021, Fiserv won a Nest Bank contract to provide transaction monitoring and data analyses to help ensure transaction security, identify suspicious transactions, and eliminate scams and fraud.

- Fast Company named Fiserv one of World's Most Innovative Companies 2021 – Fiserv being recognised as 'turning challenges into impact-making processes.'

- New York Community Bank has also selected Fiserv's DNA solutions, amongst others, in 2019.

- Fiserv has enabled American Family Insurance, (a Fortune 300, multi-line insurance company) to accept payments via more than 30,000 CheckFreePay locations in the US. The partnership provides in-person cash payments to be made, conveniently and securely. CheckFreePay from Fiserv gives customers the option to make insurance payments via cash in the same places they shop, eg, major retailers, which offered greater convenience during the COVID-19 pandemic.

iv. High-level View of Products

The Fraud Risk Management solutions portfolio from Fiserv provides fraud prevention and AML software for banks, insurance companies and casinos using real-time behavioural risk monitoring and advanced analytics to deliver superior results.

In March 2015 Fiserv launched four next-generation solutions in this portfolio, all delivered on a common technology platform called the Financial Crime Risk Management Platform. These solutions are:

- AML Risk Manager: Delivering predictive analytics and visualisation, behavioural profiling of any entity, real-time transaction monitoring, the ability to quantify risk mitigation through investigation and beneficial ownership insight with user configurability. The solution includes Foreign Account Tax Compliance Act and sanctions screening (including SWIFT).
- Payment Fraud Manager: Delivering real-time responses using predictive analytics and scorecards to focus fraud investigators on the highest risk electronic payment transactions.
- Check Fraud Manager: Using predictive analytical models built on millions of examples of cheque transactions and incorporating signature analytics and real-time decline capabilities for items presented at the cashier window and via Remote Deposit Capture.
- Customer Risk Manager: Delivering customer-level profiling and risk scores based on predictive indicators and non-financial event information to detect relevant changes in a customer risk profile; increasing fraud detection effectiveness and reducing false positives.

The four solutions incorporate real-time behavioural risk monitoring, new advanced inference capabilities, including predictive analytics, real-time profiling of entities related to a financial services product and user-configurable rule and strategy creation.

Fiserv offers both hosted and on-premises solutions for its fraud risk management solutions.

- FraudNet is a centralised fraud detection and integrated case management system, that scores online bill payments and stops bill processing if a suspicious transaction is spotted. The data from this transaction is sent to fraud specialists to review. The FraudNet engine uses advanced algorithms and proprietary negative file history; making it extremely accurate in detecting fraudulent transactions before they are processed.
- FraudNet analyses high-volume data streams, detecting complex suspicious scenarios and examining behavioural patterns, and provides the real-time intelligence necessary to identify fraudulent transactions.

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- Fiserv has an extremely strong brand and market presence in financial services. The company is global and the merger with First Data has only strengthened this position. The company has been recognised as one of the most innovative in the industry.
- Fiserv's strong portfolio of products covers a wide spectrum of use cases.
- Strong partnerships with organisations such as Main Street Insights (formerly Clover Insights) widens Fiserv's portfolio of solutions into the small retailer world.

4.4.8 GBG

Juniper Research interviewed Laura Barrowcliff, Head of Strategy and David Mirfield Financial Crime and Risk Manager at GBG and Eric Leiserson, VP Research and Marketing, IDology in March 2021.

i. Corporate

GBG PLC was founded in 1989 and employs more than 1,000 people across 16 countries. The company has 20,000 customers in 70 countries. Customers include eBay, Lego, Santander Bank, and BNP Paribas.

GBG PLC is a global specialist in identity data intelligence; specialising in the use of data to verify individuals and to mitigate fraud. GBG PLC added significantly to their portfolio in 2019 with the acquisition of fraud prevention company, IDology, for a reported $300 million.

Chris Clark is CEO and Nick Brown Group Managing Director.

Figure 4.9: GBG PLC Financial Snapshot (£m/$m), 2019-2020

	2019	2020
Total Revenue	£143.5/$200.2	£199.1/$277.7
Operating Profit	£47.9/$66.8	£32.0/$46.6

Financial Year End 31 March Source: GBG PLC

ii. Geographic Spread

The company has offices in 16 countries across EMEA, APAC, and the United States. GBG PLC is headquartered in Chester, in the UK.

iii. Key Clients & Strategic Partnerships

GBG PLC relies on a data network that has global reach. They use data from 150 partnerships with public and private sector data providers.

During 2020, key strategic partnerships were created:

- Group-IB: A leading provider of solutions aimed at detection and prevention of cyberattacks, online fraud, and IP protection.
- Revolut: GBG PLC and Revolut partnered to deliver safe digital services using KYC and AML.
- Emailage (part of LexisNexis Group) uses email intelligence to profile risk levels.
- CredoLab: GBG PLC made a strategic investment in Credolab, which uses alternative data sources to generate risk scores.

iv. High-level View of Offerings

GBG PLC has three core product areas:

- Location Intelligence: Including address capture and verification – GBG PLC has seen a lot of interest from eCommerce in 2020.
- Identity Verification: Including biometric, document and age verification; GBG PLC has a global solution with regional offerings in EMEA, APAC and the US.

- Fraud and Compliance Management: Including application fraud, transaction monitoring, and AI-enabled fraud detection.

‘GBG PLC is increasingly seeing the identity and fraud worlds collide. The identity and fraud propositions are about understanding identities, but also whether you trust that identity and what is the 360-degree view you have of it. A growing use case is as payments change and become more digital, there is an additional need for fraud detection.’ – Laura Barrowcliff, Head of Strategy, GBG PLC

GBG PLChas a priority to ensure a consistent user experience across their three tracks that then fits with a 360-degree model where identity and fraud merge. The ML models it deploys automatically retrain on the data in the system to keep them abreast of changing fraud threats. Customers can use a ML toolkit to take production data and develop statistical features and build their own models.

The identity verification portfolio is used to verify users in several sectors, including, most notably, gaming. GBG was also involved in the UK government’s Verify citizen identity initiative, using the brand name CitizenSafe, until 2018.

‘Layering and fusing physical with digital attributes and transparency of data, along with customisability, is a unique aspect of the GBG PLC solution set. Identity verification – can see the fraud that takes place, the real-time learning models we use provide a very powerful tool for fraud mitigation. It does not stop at the point of fraud event. There is a post-management team to provide alerts. This is on a global basis.’ – Eric Leiserson, VP Research and Marketing, IDology

The GBG ID3global platform uses data from multiple sources; exposing it through an API interface. The platform can be used for a variety of identity verification checks such as KYC, PEPs and Sanction checks, age verification and bank account verification. ID3, has unique matching capabilities, that allow it to identify more than 90% of individuals during the application process. It can check the authenticity of identity documents including, passports, driver's licence or electricity bill, instantly.

ID3 is accessed via a web portal or directly integrated; using web services, into existing applications. ID3 can be deeply integrated into a user journey, and customers can set the pass or fail mark with ID3 producing a set of results, based on this specific profile which can indicate whether the application should be accepted, rejected or referred back to the customer for further information. This defines, from a risk perspective, what an acceptable end consumer or individual looks like. These rules are then built into the decision-making process to create a score for each ID3 check. This score can be weighted to support any risk-based approach or customer requirements.

The GBG PLC fraud and compliance solution portfolio has a number of products that cover areas across the payments and anti-fraud surface:

- Predator provides real-time fraud protection. It uses scoring algorithms across touchpoints to provide alerts when suspicious activity is spotted. Behavioural analytics is used to create a baseline set of activity for an individual. The solution works across a multi-channel payment setup to monitor transaction channels such as digital wallet, Internet banking, credit card or contactless payment.

- Instinct Hub is a compliance and fraud risk management platform. It is designed to work across an omnichannel customer journey during the account opening and application process.

It increased fraud detection accuracy by 30%. Instinct is used to verify an applicant's official and biometric identity, and locate potential email, phone, device or endpoint security vulnerabilities.

The GBG PLC GreenID product is used to authenticate a user's identity. It is based on verifiable credentials, such as identity documents and biometric data. It works across multiple channels, and uses large datasets to validate a user identity, including PEP and AML checks. GreenID is applicable to fraud related to identity theft.

Figure 4.10: GreenID

Source: GBG PLC

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- GBG PLC has built its portfolio of products to cover an identity-related approach to financial crime. The deep integration of IDology technology has added a layer of innovation that gives GBG PLC a unique position in the space. Its attention to the omnichannel/customer lifecycle, including the identity aspect of this lifecycle, makes them a formidable competitor.
- In positioning itself as an identity-focused solution, GBG PLC is central to resolving an increasingly complex identity data problem. The use of a hub-based approach to orchestrate its many datasets, provide an excellent backbone for risk-reduction during the onboarding process. Their use of machine learning to analyse this data adds to the probability scoring during verification. Synthetic identity is also tackled using this approach.
- Their platform is designed to allow for deep integration across omnichannels. This is a benefit in a consumer space where customer will use multiple channels for purchases.
- GBG PLC could potentially use Open Banking to add additional data/validation/KYC options to their platform.

4.4.9 Kount, an Equifax Company

Juniper Research interviewed Vikram Dhawan, Vice President and Senior Product Leader, Rich Stuppy, Vice President and Senior Customer Experience Leader, Kount in March 2021

i. Corporate

Kount, founded in 2007, is a leading fraud prevention solution provider. It has built a solution that focuses on AI, machine learning and identity trust to provide the complete fraud solution.

In January 2021, Kount was acquired by Equifax for $640 million. A press release by Equifax on the acquisition stated that:

'The combination of Kount solutions with Equifax differentiated data assets and cloud capabilities will enable us to quickly take advantage of new fraud prevention and digital identity offerings to deliver for our customers and drive Equifax growth. Our strong 2020 financial performance and balance sheet allowed Equifax to reinvest our outperformance in Kount, while continuing to look for attractive acquisitions to strengthen our data assets and solutions.'

Kount is led by Bradley J Wiskirchen (General Manager and Senior Vice President); Jim Gasaway (Vice President and Senior Technology Leader); Rich L Stuppy, (Vice President and Senior Customer Experience Leader).

ii. Geographic Spread

The company is based in Idaho, US, with a global customer base. Kount has over 30 patents, and 9,000 brands as customers. They handle over 32 billion interactions to build the Identity Trust Global Network. Kount can take advantage of the massive Equifax dataset of signals.

'Bringing the physical and digital together is the only way to create a comprehensive view of identity and track it through a fraud lifecycle' – Vikram Dhawan, Vice President and Senior Product Leader, Kount

'In terms of success rates, each customer is different, but case studies see 90% reduction in chargebacks, 100% reduction in review, all key KPIs across all of our 9,000 customers see consistent execution against these KPIs.' – Rich Stuppy, Vice President and Senior Customer Experience Leader, Kount

iii. Key Clients & Strategic Partnerships

- Equifax is now the owner of Kount.
- The company brings to Equifax, over 9,000 global brand customers across the world.
- Kount has a network of data partners, including Verifi (Visa), Ethoka, Ekata, and more.

iv. High-level View of Offerings

Kount's has a portfolio of products built around the payments' arena and fraud and risk management. The solution includes a set of key APIs:

- Device collection API that collects information from the device.

- Transaction API that collects all sorts of different data – this utilises AI and ML, a policy engine, a portal, a data analytics tools and access to all the data used to make decisions (Data on Demand).
- Response and Synchronisation API for orchestration purposes.

Kount Command: The solution uses AI to reduce digital payments fraud, protects against chargebacks, and delivers personalised customer experiences. Command uses a large network of trust and fraud-related signals analysed using machine learning. This ML is used at both the macro and individual level to assess trends.

Kount Control: An account takeover prevention tool. Control provides adaptive authentication against ATO attacks, and offers policy customisation to fine-tune protection, and reporting/data presentation to uncover trends. It reduces false positives, enables customised user experiences, and reveals trends that enrich custom data to inform future policies.

Data on Demand: A private data warehouse that enhances a company's customer knowledge with thousands of additional data points from Kount's Identity Trust Global Network. This data crosses different transaction complexities, different verticals and different geographies, so machine-learning models can be properly trained to accurately forecast risk. This provides merchants, regardless of industry, customer base, or geography, the insights they need to protect against fraudulent activities.

a) Advanced AI & Machine Learning

Kount's AI combines extensive unsupervised, as well as supervised, machine-learning models. These models are shaped with over 13 years of deep domain expertise and trained on data from Kount's Identity Trust Global Network.

The company has extensive fraud expertise, with a team of data scientists determining the most meaningful machine-learning feature types of attacks. This also enables the ability to use those features to identify behavioural anomalies.

Kount uses both supervised and unsupervised in a symbiotic way to help build better and more current models. Kount uses real-time unsupervised machine-learning to look for linkages and anomalies and leverage the network to create features that are fed into the supervised machine learning. This learns over time, based on historical behaviour to create a real-time Omniscore.

The Omniscore is part of a transparency approach, clients also get the policy engine and the many signals the Omniscore is based on. This allows the client to understand the decisioning process.

Figure 4.11: Kount Decisioning Process

Source: Kount

b) Customer Experience Engine

This provides the ability for customers to fine-tune fraud prevention decisions, conduct investigations and monitor performance seamlessly.

Customer Experience Engine enables customers to create rules and policies that meet their unique business needs (from promotions and policy abuse to non-fraud chargebacks) and to customise their risk thresholds to address emerging attack methods, new use cases and issues, such as bad marketing affiliates and SKU-specific policies.

That knowledge can lead to improved marketing activities, the introduction of new use cases, or the expansion of sales channels. The analysis possible with Datamart goes far beyond preventing fraud behaviours to providing insights into business performance.

The combination of these different elements gives Kount a convincing platform in the FDP space.

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- Kount's portfolio of AI-driven antifraud solutions made it an attractive purchase for Equifax. This acquisition will allow Equifax to establish itself alongside competitors such as TransUnion and Experian.
- Kount has been agile in its development of leading AI-driven products. If it continues to innovate around identity-led financial crime, it will be a force in the market and add enormous value to Equifax.

4.4.10 LexisNexis Risk Solutions

LexisNexis® RISK SOLUTIONS

i. Corporate

ThreatMetrix was founded in 2005 as a small, venture capital-backed company which develops and markets SaaS-based FDP solutions. The company launched its first authentication products, which catered for eCommerce and social media companies, in 2009.

LexisNexis Risk Solutions and Accuity merged operations, with the latter becoming part of LexisNexis Risk Solutions Group. Of the merger, Rick Trainer, CEO of LexisNexis Risk Solutions, said in a press release:

'Accuity is an excellent strategic fit for Business Services. Both companies share a common vision – enabling financial transparency and inclusion around the world using innovative technology and comprehensive data to help our customers control risk, enhance and empower compliance and optimise business processes.'

In 2020, LexisNexis acquired ID Analytics, a San Diego-based provider of fraud and credit risk solutions. ID Analytics utilises advanced technology, data and analytics to deliver actionable insights for enterprises.

In 2020, LexisNexis bought Emailage, an expert in global email intelligence and enhanced predictive risk scores.

In January 2018, the RELX Group (owners of LexisNexis) announced its intention to acquire ThreatMetrix for £580 million ($742 million) in cash. The deal was closed in February 2018. As part of the acquisition,

ThreatMetrix has become part of the RELX Group's Risk & Business Analytics segment, which includes LexisNexis Risk Solutions. In late 2019, LexisNexis released a statement that ThreatMetrix would be known as LexisNexis Risk Solutions.

Key executives at the company include Mark Kelsey (CEO, Risk & Business Analytics division of RELX); Rebecca Schmitt (EVP and CFO Risk and Business Analytics division of RELX); Vijay Raghavan (EVP and CTO Risk and Business Analytics division of RELX).

RELX is also owner of Accuity.

Mark Kelsey is CEO, and Vijay Raghavan is Executive Vice President and CTO.

Figure 4.12: RELX Group Financial Snapshot (£m/$m), 2019-2020 (reported figures, non-adjusted)

	2019	2020
Revenue (£m/$m)	£7,874/$10,921	£7,110/$9,861
Risk (£m/$m)	£2,316/$3,212	£2,417/$3,352
Net Profit (£m/$m)	£1,505/$2,087	£1,224/$1,698

Source: RELX Group

Please note the currency was converted at rate on 20th March 2021.

ii. Geographic Spread

LexisNexis Risk Solutions headquarters are in Georgia, US. The company has additional offices in New York City, Hong Kong, Sydney, London, Paris, Tokyo and Amsterdam.

iii. Key Clients & Strategic Partnerships

- Most of LexisNexis Risk Solutions business involves supplying its core digital identification data to a number of customers around the world. These customers use this digital ID data as one layer of coverage and incorporate it into their own analytics and fraud resolution systems.
- LexisNexis Risk Solutions has a number of very large customers, such as Cybersource, which uses its digital identification data. Other eCommerce partners include Accertify, ACI Worldwide, Cardinal Commerce, First Data and LexisNexis.

iv. High-level View of Products

LexisNexis Risk Solutions online payment fraud detection platform is known as the CyberCrime Protection platform. This allows businesses to profile devices and identify threats, examine users' identities and activity, as well as configuring business rules and generate analysis and reports. LexisNexis recognises that robust verified identity plays a central role in fraud prevention.

The platform protects against account takeover, payment fraud, fraudulent account registration, multi-channel web fraud and remote workforce access resulting from malware and data breaches. It can be used in a variety of verticals, including financial services, enterprise, eCommerce, government and insurance. LexisNexis Risk Solutions also targets some niche markets, such as online lending, games and online gambling.

The core technology in the CyberCrime platform is digital identification; it uses a number of processes to detect and establish a complete risk profile for a transaction, including:

- Fraud Intelligence is a 2021 addition to the LexisNexis portfolio and is a result of the acquisition of ID Analytics. The tool is designed to help organisations mitigate new account fraud risk. The tool detects real-time fraudulent applications. It is able to achieve this using ML; analysing hundreds of unique identity characteristics and identity application behaviours. The tool works by generating a fraud risk score, serving as an indicator that a specific fraud risk requires further investigation.
- LexisNexis Emailage was launched in 2020 as a part of the strategic acquisition of the company of the same name. The tool is a fraud risk scoring solution that uses email to achieve a seamless user experience with robust fraud detection and prevention capabilities.
- LexId Digital identity verification is a cornerstone of how LexisNexis deals with fraud. The LexId Digital solution sites at the centre of the LexisNexis Digital identity Network. This provides a 360-degree view of customers using both offline and online data to establish verified digital identities. It can also detect synthetic and stolen identities, as well as unusual behaviour.

The previous acquisition of ThreatMetrix which brought digital identity intelligence and authentication powered by insights from billions of transactions and embedded machine learning under the organisation's umbrella has created a formidable company that has a strong focus on the use of data to manage fraud, based on identity data-based transactions.

LexisNexis Risk Solutions profiles over 1 billion transactions monthly and protects more than 250 million users' accounts for 3,000 customers and 15,000 websites. Individual threats such as malware, excessive login attempts, suspicious geolocations, dubious connection paths and hundreds of additional anomalies are detected and recorded.

Most of LexisNexis Risk Solutions business is associated with its core device profiling and threat identification technology, which the company offers to other FDP solutions providers, which use it as one layer of coverage.

The company only has a SaaS-based hosting option. It is predominantly known as a data feed or datapoint provider. However, LexisNexis Risk Solutions has now developed a complete FDP platform, still cloud-based, which incorporates decision analytics, case management and other solutions typically offered by its much bigger, established rivals.

v. Juniper's View: Risk Solutions Key Strengths & Strategic Development Opportunities

- LexisNexis Risk Solutions has become even stronger with the strategic merger and acquisition of complimentary and symbiotic technologies. This consolidation of key technologies into the LexisNexis stable creates a strong market leader and Juniper Research expects this strength to show keenly in the coming years.
- The company's expertise in data analysis can help with strategic product development as new cybersecurity issues arise.
- LexisNexis Risk Solutions is cloud based, meaning there is no software or hardware to install. The company is regarded as very cost-competitive and it offers a number of flexible options, particularly suited to smaller merchant companies. These include flat rate charging options, ie tiered fixed dollar charge per month, depending on the number of transactions analysed.

4.4.11 Microsoft

Juniper Research interviewed Kapil Tandon, Core Product Lead, Anand Oka, Partner Group Program Manager and David Sarjantson, Senior Director, Microsoft in March 2021

i. Corporate

Microsoft was founded in 1975 and is based in Redmond, Washington, US. The company employs around 168,000 with around 60% of those employed in the US. The number of employees has increased by about 14% since 2019. Microsoft is traditionally recognised for its software products such as operating systems and Microsoft 365 applications. However, the company also has a tradition in developing security and identity-related products, with Active Directory going back to 1999. In January 2021, Microsoft announced that its Security, Compliance, Identity and Management business exceeded $10 billion annual revenue and grew 40% year-on-year. Microsoft recently launched capabilities to protect against payment, account, returns and discounts fraud.

Key executive members include Satya Nadella (CEO) and James Phillips, (President, Digital Transformation Platform Group).

Figure 4.13: Microsoft Financial Snapshot ($m), 2019-2020 (reported figures, non-adjusted)

	2019	2020
Revenue ($m)	$ 125,843	$143,015
Net Profit ($m)	$44,281	$52,959

Source: Microsoft

ii. Geographic Spread

Microsoft is headquartered in Redmond, Washington, US. The company has offices across the globe. The company employs over 168,000 people, with almost 50% of them working in engineering roles.

iii. Key Clients & Strategic Partnerships

- Microsoft runs a successful partner programme (Microsoft Partner Network, MPN) of around 64,000 solution providers and vendors. Microsoft builds its security products to integrate into the wider security ecosystem.
- Capital One: In 2020, Microsoft and Capital One partnered to provide a cloud-based authorisation engine that improves fraud detection accuracy.

iv. High-level View of Products

- Microsoft Cloud for Retail is available in public preview - Microsoft Cloud for Retail brings together different data sources across the retail value chain and uniquely connects experiences across the end-to-end shopper journey through a set of capabilities that deliver more relevant personalised experiences and operational excellence for sustained

profitability. The solution integrates existing and new capabilities in Microsoft 365, Azure, Dynamics 365, and Microsoft Power Platform, the company using the partner ecosystem to build on the platform and add capabilities required for delivering seamless experiences across the shopper journey in Retail including loss and fraud prevention.

- Microsoft Cloud for Financial Services - had a public preview on 31st March 2021. This is a new product from Microsoft to cover the end-to-end needs of complex control frameworks and regulatory requirements. The solution integrates existing and new capabilities in Microsoft 365, Azure, Dynamics 365, and Microsoft Power Platform, the company using the partner ecosystem to build on the platform and add capabilities required by the financial services industry, including anti-fraud options – the platform includes analytics for modelling, insight, and regulatory reporting.

- Microsoft Dynamics 365 Fraud Protection is the main fraud detection capability offered by Microsoft. The company originally built a solution for its own merchant ecosystem but soon realised it had wider potential. The solution covers a wide remit of payments and transactions including online and in-product purchases, Azure cloud services, Office subscriptions, and invoice-based purchases. Microsoft Dynamics 365 Fraud Protection helps eCommerce, brick-and-mortar, and omnichannel merchants protect their revenue. Dynamics 365 handles over 1 billion transactions per year with 760 million MAU. The KPI improvements for organisations using Dynamics 365 include an 82% reduction in manual reviews, with false positive rates decreasing by 132 bps (Basis Points). (Please note that 1% = 100 bps).

The full customer journey is an important remit in the application of Dynamics 365, including post-purchase such as ineligible returns. The product works across three areas:

- Account protection: Protecting against bots, account takeover, fraudulent account creation, and credential stuffing/brute force attacks.
- Purchase protection: Reducing fraud and improving acceptance rates by balancing revenue opportunity vs fraud loss.
- Loss prevention: Mitigating losses from illegitimate returns and discounts across multiple channels.

To achieve these three core protections the system uses a number of core technologies:

- Adaptive AI-enabled models.
- Behavioural analytics generated from its own fraud networks across their wide customer base.
- Device fingerprinting.
- Bot protection.
- Account creation and sign-in protection, to help mitigate credential stuffing and synthetic identities.
- Decision engine for specialised rules and policies.

The balance of usability via friction-free experiences against fraud prevention is an important aspect of the solution. The mix of the core

technologies reduces wrongful rejection combined with account protection builds better customer experiences and helps maintain retailer reputation. Omnichannel purchase protection helps merchants to identify potential fraud on returns and discounts. For example, a customer buys an item at a discount online then returns to the store requesting a full price refund.

The vast footprint that Microsoft commands via their customer base is used to help train the AI algorithms. The use of adaptive AI allows the models to adapt to new fraud patterns in real-time.

'We are both a large merchant that has to protect our own commerce environment, and a solution provider. With Dynamics 365 Fraud Protection – a cloud-based solution that helps protect merchants' revenue and reputation – we use adaptive AI to detect where fraud is happening and mitigate it through a variety of product capabilities.' – David Sarjantson, Senior Director, Microsoft

v. Juniper Research's View: Risk Solutions Key Strengths & Strategic Development Opportunities

- Microsoft built its FDP platform for its own and its vast array of merchant use. This starting point has given the company a unique perspective, allowing it to build features for this marketplace that are transferable outside of the Microsoft vendor ecosystem.
- Microsoft recognises that the entire lifecycle of the transaction provides potential for fraud. Currently, it does not integrate KYC technologies in the account protection area of Dynamics 365. This may be coming down the line at some point, in which case the solution will be truly holistic.
- Microsoft is an outlier in an industry that is dominated by certain players, also known as, heavyweight FIs or CRAs. This could work in Microsoft's favour as it reaches out to their established user base and uses this as a way to outcompete these established FDP players.

4.4.12 NICE Actimize

NICE · ACTIMIZE

i. Corporate

Based in Israel, NICE was founded in 1986 and develops solutions to help financial compliance and financial crime prevention, as well as services to improve customer engagement. The company's fraud detection solutions operate through a wholly owned subsidiary, NICE Actimize.

Nice Actimize acquired Guardian Analytics in 2020 to strength Actimize's presence in in the small- to medium-sized enterprise market. In a press release the company stated that:

'The acquisition of Guardian Analytics brings together the unique combination of proven expertise, best-in-class innovation, and the power of the cloud, presenting a major opportunity for accelerated growth. […] Fraud and anti-money laundering capabilities will empower firms of all sizes to accelerate the adoption of the industry's most innovative solutions.'

Figure 4.14: NICE Financial Snapshot ($m), 2018-2019

	2018	2019
Revenue	$1,444.5	$1,573.9
Financial Crime & Compliance Revenue	$288.4	$308.8
Operating Income Financial Crime & Compliance	$109.5	$124.7

Source: NICE

Key executives at NICE Actimize include Craig Costigan (CEO); and Chad Hetherington (VP and Global Head of Product).

ii. Geographic Spread

NICE operates from offices located in five continents across the globe.

iii. Key Clients & Strategic Partnerships

- NICE operates a scheme of technology, business and global alliance partners. Key brands include Accenture, Bain, Boston Consulting Group, Cisco, Cognizant, ConvergeOne, Deloitte, Fuze, IBM, Infosys, IPC, Motorola, PWC, RingCentral, Salesforce.com, Servion, Tata Consulting Services and Verizon. Integration with NICE's technology is facilitated by the DEVone programme, which includes over 100 partner companies.
- The X-Sight Marketplace, the industry's first financial crime management ecosystem, was developed by NICE Actimize. In late 2019, The Data Initiative and Financial Intelligence & Analytics partnered with X-Sight Marketplace. The platform is looking to improve 'data processing including curating public domain information for AML, as well as SWIFT and ACH message translation.' It has over 60 vendor partners.
- NICE has a very broad customer base, with 25,000 organisations in more than 150 countries on its books, including over 85 of the Fortune 100.

iv. High-level View of Products

NICE offers a cloud-native open platform that covers Customer Engagement and Financial Crime and Compliance offerings. Its product ethos is one of adaptation that reflects customer experience, according to needs and behaviours. This approach allows the technology to drive a 'proactive approach to identify intent' providing a basis for prediction and protection, as well as mitigating compromised accounts and events. Analytics, AI and automation based on machine learning are the core technology underpinning this. Large datasets are used to train the ML algorithms via the cloud offering. NICE Actimize delivers a portfolio of solutions to provide protection against digital fraud. These are delivered via a core platform, which uses a modular design to incorporate the services outlined below:

NICE Actimize solutions that come under NICE's Financial Crime and Compliance solutions, are based on a single core platform that enables financial services organisations to expand the use of NICE's solutions over time.

- X-Sight, is a cloud PaaS for Financial Crime and Compliance solution.
- AFCM (Autonomous Financial Crime Management): Merges data, analytics and automation technologies. Raw data is used to generate actionable intelligence by applying machine learning, advanced analytics and automation. The solution allows organisations to support both semi-autonomous and fully autonomous operations.

The solutions are based on:

- Analytical models and flexible tools: The core platform uses analytical models and tools to develop and customise analytical models, data sources, and business processes at both the business and IT levels.
- Multi-channel management: The solutions are proven to capture and analyse thousands of financial transactions a second, across multiple channels.
- Behavioural analysis: The tools can be used to detect anomalous customer or employee behaviour in real-time.
- Real-time decisioning and enforcement: A real-time decisioning engine uses analysed data to trigger alerts. Workflow and investigation allow effective alert management.

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- NICE Actimize offers a very broad solution that is highly tailored to the financial services industry. Their range covers multiple channels, important in a world where customer expectations are diverse and channel options are a vital ingredient in user choice.
- The use of machine learning with an emphasis on workflow management and semi-autonomous alerts means that Actimize can deliver solutions that are attractive to the analyst team, as well as the commercial team.
- The use of X-Sight as an ecosystem, will allow Actimize to become a central pivot in the wider payments' fraud space and create useful synergistic relationships to open new commercial channels.

4.4.13 NuData Security

Juniper Research interviewed Robert Capps Vice President Emerging Technologies, NuData in March 2021

i. Corporate

NuData was founded in 2008. Its core focus is on biometrics and behavioural analytics, which it uses to identify legitimate users and prevent fraud.

In March 2017, Mastercard announced that it would acquire NuData as part of its effort to broaden its FDP portfolio. The terms of the deal were not disclosed. Mastercard has a separate section in its operations known as Cyber and Intelligence. This section incorporates threat scanning using AI.

Key executives at NuData include Robert Capps (VP Emerging Technologies); Randy Lukashuk (CTO); Michelle Hafner (Senior Vice President, Product Strategy & Execution).

Mastercard has an increasing focus on digital identity and, in 2019, introduced its 'vision for digital identity in today's increasingly connected world.' It has since announced an investment of $510 million to build a centre for innovation in digital and cybersecurity, AI, and the IoT, called the

'Intelligence and Cyber Centre.' Mastercard works with a number of key strategic partners to forward this focus. This includes FIs and banks, as well as the application of Open Banking, to work towards verified identity transactions. This is Mastercard's sixth global technology centre and its first in Canada. NuData is expected to play a key role.

Figure 4.15: Mastercard Financial Snapshot ($m) 2018-2019

	2018	2019
Revenue	$14,950	$14,950
Net Income	$5,859	$16,883

Source: Mastercard

ii. Geographic Spread

NuData operates from its headquarters in Canada. Mastercard offices are in six continents around the globe.

iii. Key Clients & Strategic Partnerships

- NuData has established partnerships with vendors such as Accertify, Early Warning and Amazon Web Services, as well as NAORCA (National Anti-organized Retail Crime Association). It also partners with Zelle and Jack Henry & Associates.
- NuData uses strategic partnerships to build inroads using synergistic technologies. Recently, this included the Entersekt Secure Platform built on multi-patented customer authentication and endpoint security technology. Central to the system is digital certificate-based consumer device ID, seamlessly transforming mobile apps and desktop browsers into regulatory compliant second factors of authentication.
- NuData's clients include two of the largest banks in the world, as well as five of the largest ten global eCommerce companies.
- NuData's solutions are now available through the AWS PrivateLink and fully supported for AWS customers.

iv. High-level View of Products

At the heart of the company's offering is its behavioural analytics solution, NuDetect. This solution is fundamentally focused on identification of genuine users at an early stage and throughout the user journey. In this manner, friction during the transaction or service is reduced; providing a better consumer experience. NuData's approach to fraud detection is multi-layered and consists of:

- NuDetect for Continuous Validation – covers the user journey from login to logout. Uses a mix of behavioural analysis and biometrics, large datasets and machine learning are used to spot anomalous events.
- Device identification – including data surrounding the connection and location. Traditional authentication methods, such as username and password can be used here, but data compromises are safeguarded through implementation of mechanisms such as MFA, behaviour and other data that can be associated with the device.

- Analysis of user behaviour on the website or in app – here, the manner in which the user navigates the site, enters information into fields and so on is monitored against known 'good' behaviour.
- Analysis of biometric indicators – while fingerprints, iris scanning or voiceprints are commonly thought of as biometric indicators, NuData also draws on information from other, more passive data sources, such as the gyroscope, accelerometer and other settings that are likely to be unique to the user.
- Verification against a Trust Consortium of cloud-based data and entity links – fraudulent activity and entities are registered here and can be used to identify organised crime rings and collective fraudulent behaviour.

The effectiveness of the NuDetect platform is augmented through analysis, comparison and aggregation of intelligence from other sources. The solution is active throughout the lifecycle of the end-user's interaction with the site or app, with data collected at the point of account creation, through login and ending with the transaction. In turn, this enables NuData to offer FDP in terms of synthetic account creation, account takeover, automation detection and online payment fraud.

'NuData works to mitigate the massive high-volume attacks that happen on a large scale across payments. However, these mass-attacks are often used to take attention away from the more nuanced attacks. NuData provides protection against both large-scale attacks and emerging threats. […] NuData has top five banks as customers in most regions around the world, they are the 'canaries in the coal mine' for new attacks. AI, specifically unstructured learning can identify patterns that may not stand out to human fraud analysts, these can be used to identify anomalous patterns so we can reverse engineer the attacks. Understanding the way attacks happen and orchestrating a user process so that a good consumer will be able to walk through the process without additional friction is NuData's remit.' – Robert Capps, VP Emerging Technologies, NuData

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- Mastercard's ownership of NuData is major positive factor, meaning that it has access to a wide network of transactions. It also has a very wide partner network, which further enhances these abilities.
- NuData has significant machine learning capabilities, with other machine learning coming from Mastercard, including transaction monitoring at Vocalink. Its machine learning credentials are therefore more robust than others. The Mastercard connection provides a massive data source for ML analysis.
- The application of validation checks across the user journey (continuous validation) allows NuData technology to be deeply embedded and manage friction – this balance will work in NuData's benefit in an increasingly online market. The trick for NuData to maintain dominance in this area is to be inclusive and cover all possible channels and user journeys; incorporating Open Banking as a validation point may benefit under certain scenarios.

4.4.14 Riskified

riskified

i. Corporate

Riskified, founded in 2013 in Tel Aviv, Israel, is a provider of eCommerce FDP solutions.

The company has raised six rounds of funding to date, a total funding amount of $228.7 million. The most recent, Series E funding was announced in November 2019. This raised $165 million and involved Pitango Venture Capital, General Atlantic, Entrée Capital, Fidelity Management & Research Company and Qumra Capital.

Riskified was founded by Eido Gal and Assaf Feldman.

ii. Geographic Spread

Riskified is based in Tel Aviv, Israel. In 2016, the company opened its first international office in New York, USA.

In 2020, Riskified opened an office in Shanghai.

iii. Key Clients & Strategic Partnerships

- Riskified has an extensive list of eCommerce customers, including Wish, Mattel, Aldo, Canada Goose, Prada, Last Minute, Ring, United Colours of Benneton and many others.
- The company also has an extensive partner ecosystem, including Salesforce, Moku, Bvaccel, Banca Sella, Stripe, Shopify and Checkout.com.
- Air Europa chose Riskfied for a seamless, friction-reduced booking experience.

iv. High-level View of Offerings

Riskified's offering is made up of several different key elements with a focus on the needs of smaller retailers:

a) Account takeover prevention

Account Protection by Riskified enables eCommerce vendors to stop bad actors from taking over accounts, exploiting loyalty programmes and abusing sales promotions. This solution uses AI to differentiate between good and bad actors.

b) Payment Authorisation

The solution enables vendors to minimise PSD2's negative impact on the customer experience, by routing exempt orders outside this process. This enables eCommerce sites to remove clearly bad orders from bank review to boost their overall payment authorisation rates.

c) Dynamic Checkout

This enables vendors to dynamically change the checkout experience to match the user's analysed risk profile; offering users convenient ways to validate their purchase at checkout.

Riskified is confident enough in these elements that it can offer a chargeback guarantee, meaning that it takes full liability for every transaction it authorises, which is highly important to vendors. This is assisted by an automated representment solution, which allows Riskified to offer higher approval rates.

d) PSD2 Optimization

Riskified PSD2 Optimization uses machine learning to increase the percentage of orders that undergo TRA. The data used to optimise on PSD2 requirements is collected from Riskified's merchant network. Riskified PSD2 Optimization is the latest in a suite of AI-based solutions designed to help merchants keep legitimate customers moving along the path to purchase to prevent friendly fraud, chargeback management, and drop-offs.

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- Riskified has a highly detailed solution, tightly focused on the eCommerce arena. Its platform is performance based; retailers are only charged for approved orders. This is a very powerful feature in the SMB retailer market space as it allows an organisation to manage outgoings, following an MSP model.
- If Riskified wishes to move into a wider commercial space, it can do so by leveraging partnerships.
- The deep integration into common payment platforms, such as Magento, helps push the company further into the smaller retail sector.
- Their focus on decisions, as opposed to score, again helps smaller retailers.
-

4.4.15 RSA Security

RSA

i. Corporate

Founded in 1982, RSA has become one of the biggest names in cybersecurity over the years; offering a range of IAM solutions.

The company was acquired by EMC in 2006 for $1.2 billion, which then itself merged with Dell in 2016. In 2020, RSA was sold to a consortium of investors led by Symphony Technology Group for $2.075 billion.

Key executives include Rohit Ghai (President of the company); and Zulfikar Ramzan (CTO).

Figure 4.16: RSA Security Financial Snapshot, ($m) FY 2018-H1-2020 (YE 1st February)

	2018 H1	H2	2019 H1	H2	2020 H1
Whole Company Net Revenue ($m)	$37,115	$41,510	$44,298	$46,323	$45,278
Other Businesses	$1,010	$966	$1,153	$1,176	$1,215

Source: RSA

ii. Geographical Spread

RSA has its headquarters in Massachusetts, US, with regional headquarters in the UK and Singapore. It has a presence in nine Dell offices across Asia Pacific.

iii. Key Clients & Strategic Partnerships

- RSA runs a range of partnership programmes for both resellers and technology partners that integrate RSA products into their software. The key technology partnerships revolve around RSA's SecureID, NetWitness and Archer products.
- The SecureID platform has a wide range of prior interoperability, with over 500 apps having compatibility with RSA's authentication solutions.
- In 2020, NewDay, (a consumer credit company serving around 5 million people across the UK) selected RSA Adaptive Authentication for eCommerce, to deliver advanced fraud protection for digital payments and address the requirements of the EMV 3-D Secure protocol.
- In 2021, RSA received a significant equity investment from Clearlake Capital Group, LP. The investment made Clearlake an equal partner to Symphony Group.
- RSA's Fraud Prevention solutions are used by more than 8,000 global organisations by multiple industries, including financial services, retail, insurance, healthcare and government; it protects over 2 billion consumers. RSA partners with most of the world's largest online banking service providers leveraging an OEM model.

Figure 4.17: RSA Featured Partners

Source: RSA

iv. High-level View of Offerings

a) Identity

RSA provides a variety of identity products; providing threat detection and response through the NetWitness platform, IAM through the SecurID Suite, and Integrated Risk Management in its Archer platform. Its authentications are all in the SecurID Suite.

RSA SecurID Access provides multi-factor authentication for a range of platforms. It can leverage Touch ID, Face ID, Windows Hello and Android fingerprint sensors for its biometric sensing. This is paired with location-, device- and network-based contextual access authentication; allowing step-up authentication to be deployed as required by the client.

It also supports cloud-based SAML single sign-on capabilities through a REST-based API. The platform comes with certified interoperability for many different apps with SecurID Access.

b) Fraud and risk management

Under the umbrella name RSA Fraud & Risk Intelligence Suite, RSA provides consumer authentication and fraud protection solutions for the entire customer lifecycle, from pre-login to transaction, with omnichannel support for web, mobile, ATM, branch, call centre and IVR; offering effective omnichannel fraud protection.

The flagship solution in the portfolio is RSA Adaptive Authentication, which leverages RBA technology to detect and prevent high-risk login activity and fraudulent transactions for both the web and mobile channels.

Key products include:

- Omnichannel fraud prevention: RSA Adaptive Authentication is powered by RSA's Risk Engine. Adaptive Authentication is designed to measure the risk associated with a user's login and post-login activities, by evaluating a variety of risk indicators. Each activity is evaluated and a unique risk score between 0 and 1,000 is generated.

  Using a risk- and rules-based approach, Adaptive Authentication can prompt additional authentication via challenge questions, OOB SMS, and fingerprint and eye-print biometrics (available for mobile) for scenarios that are high risk and/or violate rules established by an organisation. This methodology provides transparent authentication for the majority of users; ensuring a positive UX.

- 3D Secure Authentication: RSA Adaptive Authentication for eCommerce is RSA's 3D Secure solution for credit card issuers and issuing processors. It enables merchants and credit card issuers to provide consumers with a consistent, secure online shopping experience, while mitigating the risk of chargeback losses.

- Adaptive Authentication for eCommerce: An RBA platform for card issuers in the 3DS ecosystem, which significantly increases fraud detection, as well as dramatically improving the cardholder experience through the elimination of passwords; protecting even more revenue by reducing shopping cart abandonment. RSA is a key stakeholder in the authentication chain for both 3DS 1.x as well as the revised protocol, through its role as an ACS provider.

  The platform has consistently high fraud detection rates of 95%, with an average intervention rate of 5% and an extremely low false positive rate. The company reports that this prevents transaction fraud, on average to the tune of $8 million per annum.

- RSA FraudAction™ is a threat management service offering attack takedown and cyber intelligence. RSA FraudAction provides organisations with complete coverage against phishing and Trojan attacks, rogue mobile apps and rogue social media pages. RSA FraudAction Cyber Intelligence service combines RSA's extensive visibility into the dark web and cybercrime underground with continuous monitoring of social media forums, to provide clients with proactive intelligence detailing threats to their organisations. 14 million markings are added to the eFraudNetwork daily, with the company reporting that the repository helped prevent $64 million in fraudulent transactions annually.

  A plug-and-play rules library is available (custom rules can be built) to help organisations identify many common high-impact fraud threats, such as Man-in-the-Browser attacks, advanced malware, vulnerability probing and business logic abuse.

RSA Adaptive Authentication offers both on-premises and SaaS-based options, depending on an organisation's individual preference. Adaptive Authentication for eCommerce is offered as a SaaS-based solution only, while RSA Web Threat Detection is offered as an on-premises solution. RSA FraudAction is offered as a fully managed external service.

RSA also has an extensive cybersecurity offering; providing cyber intelligence services in fraud, as well as in many other areas.

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- RSA has a strong brand and a highly flexible platform, that can be deployed for a variety of mobile platforms. The company has many partners, but few of these are payment providers. This means that it will be limited to larger players which will construct their own payment authentication systems.
- Investment from high-profile industry groups adds weight to RSA to help with further developments in a highly competitive space. However, there are strong growth opportunities in the industry, as cybercrime continues to innovate and move into omnichannels looking for new exploits. RSA can provide a strong merger between identity validation and adaptive authentication that will improve these omnichannel journeys, whilst protecting against common attacks.
- RSA is likely to find a strong market in the smaller retailer space as online sales take over B&M sales. Their solutions can help reduce fraud and grow CNP transaction approval rates and offer a better user experience possible. Support for the EMV 3DS protocol can also help with regulatory compliance. However, RSA must look to branding into this area as smaller retailer (and the associated hosting platforms) FDP will likely become highly competitive in the next five years.

4.4.16 SAS

i. Corporate

SAS develops business analytics software and is one of the largest independent vendors in the business intelligence market.

The company was founded in 1976 in North Carolina, US, with the original goal of developing analytical software for pharmaceutical companies, banks, academic institutions and government agencies. Today, SAS offers numerous business intelligence, analytical and statistical tools for enterprises in a wide range of verticals. According to the company's annual report, SAS invested $1 billion into the advancement of AI technology and training. In total, 27% of revenue goes back into R&D.

SAS acquired Boemska, in 2021. Boemska specialises in low-code/no-code application deployment and analytic workload management for the SAS platform. The acquisition was used to enhance SAS® Viya® the SAS cloud-native, advanced analytics that supports the entire analytics lifecycle and facilitates customer migration to the cloud.

In 2020, the company employed 13,939 people.

Figure 4.18: SAS Financial Snapshot ($m) 2018-2019

	2018	2019
Revenue	$3,300	$3,100

Source: SAS

SAS has 13,939 employees worldwide. Key executives at the company include Jim Goodnight (CEO); John Sall (Co-founder and Executive VP); Brian Harris (CTO).

The company's core future strategy will be investing in what it believes to be its core strengths including, among others, machine learning, analytics and fraud prevention.

ii. Geographic Spread

SAS's headquarters are in North Carolina, US; the company has numerous other offices in North America, South America, Europe, Asia, Africa and Australasia. They have customers in 147 countries.

iii. Key Clients & Strategic Partnerships

- SAS has numerous high-profile clients for its fraud and security intelligence solutions, including HSBC, Landsbankinn, Laurentian Bank, OTP Bank, as well as insurers such as Allianz. Overall, 92% of the Fortune Global 100 are customers of one or more of SAS's products.
- Bank of Singapore chose SAS's artificial intelligence-powered communications surveillance analytics in its training and monitoring of client representatives' performance. The surveillance framework enables the bank to monitor sales practices and align with regulatory guidelines from MAS (Monetary Authority of Singapore).
- The company operates a substantial technology, service provider and reseller network. Key partners in the FDP space are KPMG and Jack Henry & Associates.

iv. High-level View of Products

SAS has a $1 billion investment in building the future of AI and advanced analytics. SAS's main fraud product is the SAS Fraud Management Solution, a next-generation, full service, enterprise-wide fraud detection solution with the capability to monitor multiple lines of businesses on a single platform. The company targets its fraud solution at the online banking industry. Its main competitor is FICO, which dominates this segment of the market.

A new entrant to the SAS portfolio is SAS Identity 360. This solution is used across the entire user journey to prevent account takeover, detect application fraud and stop eCommerce transaction fraud. Identity and digital fraud analytics capabilities combine AI-driven data orchestration with an on-demand decision engine for real-time results.

Key features of SAS solution include:

- On-demand, real-time scoring of all transactions, including purchase, payment and non-monetary transactions.
- Analytics covers omnichannel support. A layered approach that includes cross-channel monitoring and entity link analysis; providing a holistic view of fraud.
- Sub-second response time with sustained high throughput.
- Advanced analytics, modelling platform, prediction and decision engine.

- Seamless, real-time hotlisting and integration with authorisation systems across the globe.
- Extensive rule-writing capabilities and the dynamic creation of 'public' signatures.
- Robust, flexible alert and case management for expanding customer information and decision making on multiple business lines, including monitoring of multiple accounts belonging to the same account holder.

SAS's fraud solution is offered as on-premises software and hosted SaaS solutions. There is a strong push by SAS to enable cloud analytics and for a cloud-based solution across the entire lifecycle of a user journey.

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- SAS is highly advanced in this area, as it has a much wider cybersecurity solution, which complements its position extremely well.
- Brian Harris, recently elected to the role of CTO in SAS said that the 'quiet giant' would be making more noise. This may result in a greater brand presence in the market and with the level of competitive technology in the company, this may see others being under pressure to innovate. SAS certainly spends big in the areas of AI innovation and this, coupled with a stronger brand awareness, should lead to a sales increase.[lviii]
- A push to cloud-based analytics, with the purchase of Beomska, will likely lead to upsells to their 90% on-premises user base. A more PaaS solution will allow SAS to move into new markets, including smaller eRetailers in a post-pandemic world.

4.4.17 Transunion

i. Corporate

TransUnion is a US-based company that has been in business for over 50 years. Its original remit was to provide information and insight to businesses and consumers. This remit has rapidly evolved, especially in recent years. The acquisition of CallCredit gave TransUnion a stronger UK presence. The company also targets the Philippines, Columbia, and India. TransUnion has a focus on utilising real-time data and analytics and using this within solutions that fully integrate into workflows. To achieve this, the company has made acquisitions in this area. One such acquisition was iovation in 2018. A press release at the time announced the decision allowed TransUnion to 'integrate iovation's device identity and consumer authentication capabilities into IDVision.'

Chris Cartwright is CEO.

Figure 4.19: TransUnion Financial Snapshot ($m) 2018-2019

	2018	2019
Revenue (Gross)	$2,392.9	$2,730.0
Net Income (EBITDA)	$916.9	$1,058.9

Source: TransUnion

ii. Geographic Spread

TransUnion is headquartered in Chicago, USA, and has offices in over 30 countries; employing over 8,000 people.

iii. Key Clients & Strategic Partnerships

iovation has a number of key partnerships in place, including ACI Worldwide, TransUnion, Entrust Datacard, Equifax, Fiserv, Synectics Solutions, Playtech, Scudetto, 4Stop, PassFort, Temenos, Regily, Trunarrative, Fischer, CredoLab, PingIdentity, Praxis and Threat Fabric.

High-profile clients include Confused.com, LeoVegas, Kaidee, Cashplus, Esure.

iv. High-level View of Products

TransUnion has the tag line 'Information for Good.' With this in mind, the company places data as a central component of all of its solutions and operations. Along with core consumer credit data, TransUnion add alternative data including trended credit, short-term loans, retail loans, utility, public records and digital device data.

TransUnion Shai Cohen, senior vice president of Global Fraud & Identity Solutions at TransUnion, stated in a press release:

'From the impacts of phishing and other well documented COVID-19 scams like unemployment fraud, it's clear that fraudsters have the data and increasing opportunities to create synthetic identities and utilize stolen identities.'

To combat identity fraud, TransUnion released an expanded version its Document Verification solution used to confirm a consumer's identity in faceless and in-person channels by validating a government-issued identification document like a passport or driver's licence. This product uses iovation's IDVision technology. IDVision is a data platform for reputation insights and multifactor authentication methods. It leverages over 1 billion consumer records and intelligence, based on experience with over 6.5 billion devices. IDVision integrates as a single platform solution with iovation's orchestration engine. The solution delivers alerts and reports to fraud management teams for resolution and follow-up. The platform uses of shared intelligence via IDVision with iovation's 76 million fraud and abuse reports from 35,000 websites and apps protected across multiple geographic markets; providing unique insights into industry specific fraud activities.

The TransUnion product portfolio covers three distinct areas and within that several sub-areas:

- Identity Proofing: Global ID verification/ID Document verification/Facial verification, KYC.
- Risk-Based Authentication.
- Fraud Analytics: AML compliance checks, PEP and sanction checks, device, mobile, and email validation and checks.

TruValidate is a platform that pulls together identity proofing, device risk, risk-based authentication, and fraud alerts. It can also reduce friction by pre-filling registration (and other) forms.

Fraud analytics are available via TruValidate. Machine learning device models as well as custom models are available. The models can differentiate between risky and trustworthy transactions. Synthetic fraud

models are also part of TruValidate and is used to distinguish between real and synthetic customers transactions.

v. Juniper Research's View: Key Strengths & Strategic Development Opportunities

- TransUnion's chooses acquisitions wisely; picking technology partners who have cutting-edge technology in the identity and fraud analytics space.
- The choice of acquisition of vendors, such as iovation, enable it to leverage greater resources, meaning that it can operate in a much more effective way than before. iovation's expertise in fraud detection and machine-learning models adds a new dimension to TransUnion adding a modern weight to the technology stack to give them a competitive standing.

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.cnbc.com/2020/04/29/mastercard-sees-40percent-jump-in-contactless-

payments-due-to-coronavirus.html

[ix] https://pages.blackhawknetwork.com/brandedpay.html.

[x] https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report

xi https://investor.aciworldwide.com/news-releases/news-release-details/covid-19-crisis-drives-changes-ecommerce-purchasing-behaviors

[xii] 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

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

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

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

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

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

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

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

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

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

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

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

[xxiv] 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/

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

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

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

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

[xxix] https://risk.lexisnexis.com/insights-resources/research/2020-true-cost-of-fraud-retail

[xxx] https://www.ivanti.com/lp/security/reports/2021-secure-consumer-cyber-report

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

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

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

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

[xxxv]

[xxxvi] https://www.emvco.com/wp-content/uploads/2018/12/EMV-3DS-V2.2.0-PR_FINAL-FINAL.pdf

[xxxvii] https://www.europol.europa.eu/newsroom/news/ten-hackers-arrested-for-string-of-sim-swapping-attacks-against-celebrities

[xxxviii] https://www.blackhat.com/asia-20/briefings/schedule/index.html#back-to-the-future-cross-protocol-attacks-in-the-era-of-g-18586

[xxxix] https://info.cybersixgill.com/underground-financial-fraud-2020

[xl] https://www.w3.org/2020/11/pressrelease-htr.html.en

[xli] https://www.ic3.gov/Media/Y2020/PSA200406

[xlii] https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic

[xliii] https://www.cybereason.com/blog/no-rest-for-the-wicked-evilnum-unleashes-pyvil-rat

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

[xlv] https://enterprise.verizon.com/resources/reports/dbir/

[xlvi] https://www.gbgplc.com/gbg-fraud-survey-2020/

[xlvii] https://www.linkedin.com/posts/deanjordaan_microsoft-sca-scorecard-december-2020-activity-6754842861621116928-Ag-J

[xlviii] https://www.miteksystems.com/mobile-verify

[xlix] Brundage, Miles & Avin, Shahar & Clark, Jack & Toner, Helen & Eckersley, Peter & Garfinkel, Ben & Dafoe, Allan & Scharre, Paul & Zeitzoff, Thomas & Filar, Bobby & Anderson, Hyrum & Roff, Heather & Allen, Gregory & Steinhardt, Jacob & Flynn, Carrick & hÉigeartaigh, Seán & Beard, Simon & Belfield, Haydn & Farquhar, Sebastian & Amodei, Dario. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.

[l] https://www.iata.org/en/pressroom/pr/2020-12-10-01/

[li] https://home.kpmg/xx/en/home/insights/2020/04/airlines-and-covid-19.html

[lii] https://www.reuters.com/article/us-easyjet-cyber/chinese-hackers-suspected-of-stealing-details-of-9-million-easyjet-customers-idUKKBN22V1JF

[liii] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

[liv] https://www.forter.com

[lv] Based on Accertify client data in 2021.

[lvi] https://www.featurespace.com/newsroom/featurespaces-financial-crime-viewpoint-2020-2021/

[lvii] https://www.prnewswire.com/news-releases/fico-statement-regarding-antitrust-investigation-301024452.html

[lviii] https://newsdeal.in/sass-new-cto-says-its-time-for-the-quiet-giant-to-be-loud-as-competition-increases/