ONLINE PAYMENT FRAUD

Emerging Threats • Segment Analysis • Market Forecasts
2020-2024

Reprint for Experian

First Published February 2020

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

Susan Morrow & Nick Maynard are the authors of this Work

Report Authors

Susan Morrow & Nick Maynard

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 Dynamics

1.1 Introduction

The era of the digital payment is firmly ensconced in our lives. Record numbers of online payments are being processed on all channels. Juniper Research forecasts that nearly half the world will be using digital wallets by 2024, with transaction values to increase by almost 60% to over $9 trillion in 2024. Mobile payments are a particularly important area, meaning that the industry is in the midst of a payments revolution.

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. Experian points out that 2 in 5 consumers worldwide have been victims of a fraudulent event online at some point.[i]

The legislators responded and 2019 was the year that PSD2 bedded down. However, the threat landscape has evolved significantly. Driven by omnichannel expectations and inititives that open up banking to the outside world, this landscape is pushing new challenges into the world of online payments. New entrants into the space, including Facebook's Libra, are causing a mix of consternation and awe. Libra, designed to faciliate new payments and financial service applications, may well further excacerbate the challenges as the industry deals with increasing cyber threats.

As in any other industry, disruption has potential to be a force for good; it opens up opportunities through innovation. However, online payments are not isolated, they operate in complex webs of interaction. The addition of Open Banking application program interfaces (APIs) to the mix is a key development, due to the interoperabilty and integration potential it creates. Cybercriminals know these systems well and have the ability to exploit their weaknesses. Juniper Research forecasts a $25.5 billion eCommerce transaction fraud loss in 2019, a 17% increase on 2018. By 2024, this will double to almost $50.5 billion.

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

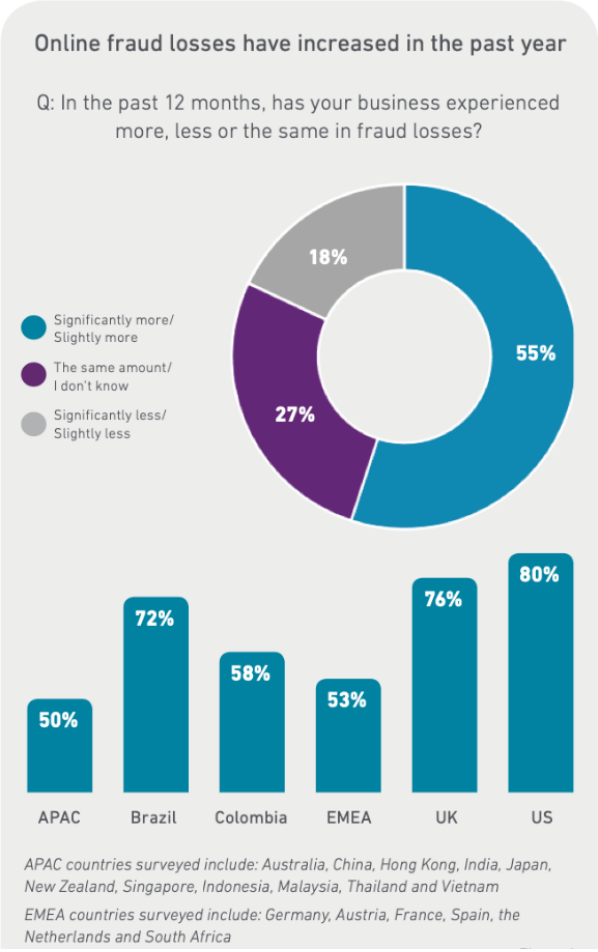
1.2 Development of Fraudulent Activity

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

According to data from Experian, 82% of businesses experienced the same or more fraud via the online channel in the 12 months prior to their "2019 Global Identity and Fraud Report" being published, with 91% of customers choosing online for goods or service purchases.[ii]

As EMV is increasingly gaining market acceptance, CNP and ID fraud is having an uptick. This is evidenced by the EMVCo's "2018: A Year in Review" showing an increasing organisational uptake of EMV by end of 2018. In contrast, Visa data shows a 76% dip in CP fraud as EMV uptake increases.[iii]

Figure 1.1: eCommerce & Fraud Attempt Growth (%), 2018-2019



Source: Experian

1.3 Key Trends in Digital Fraud

1.3.1 Fitting the Human into Payment Fraud

According to Proofpoint, 99% of cyber-attacks require human intervention.[iv] The fraudster is highly dependent at, some juncture or other in the security chain, on a human being. The human thread can be found throughout a number of key fraud activities. Fraud focusing on the CEO or other company executives is blossoming, adding a new string to the fraudsters' bow.

1.3.2 Continued Darknet Activity & Messaging Apps

i. From Darknet to Clearnet

Although there has been inroads into the closure of dark markets, which are defined as a digital market operating on the 'dark web', their replacements follow on swiftly after their demise.

Having become infamous through the rise and subsequent shut down of the initial Silk Road site, dark markets have become a relatively popular source of contraband. These include digital identities, banking, credit, or debit card information, alongside services such as carding and malware to extract sensitive information from victims.

Terbium Labs has identified the proliferation of 'fraud guides' on the darknet. These guides offer packaged instructions on 'how to commit fraud or execute specific fraud schemes.'[v] The guides are described as a way to 'crowdsource' advice; they are a training guide for wannabe fraudsters with advice on carrying out all the top fraud techniques.

Remaining anonymous on dark markets requires the use of software such as Tor and tools to transmit encrypted messages; it is further complicated by the use of cryptocurrency such as Bitcoin. This has meant that despite some success, it is relatively difficult to track down and take down these sites and fraudsters.

Whilst the darknet continues to peddle our digital identity data, financial cards and login credentials, other platforms are being used to supplement dark forces. Messaging apps like Telegram, are being used to exchange identity data and financial card details.

Research from Sixgill shows a clear move from website-based darknet markets to Instant Relay Chat and the Telegram encrypted messaging app. The company discovered 23 million credit and debit card numbers for sale using darknet methods, 15 million of which were US-issued cards. These channels offer the fraudsters automated bots which can check the validity of the cards before purchase.[vi] Research from RSA backs this finding up, a survey by the company showing a 70% growth in the volume of visible fraud activity on social media.[vii]

a) Key Takeaways

Diversification and convenience are watchwords for the fraudster community. The continued use of the darknet to propagate advice and provide the tools of the fraud trade is evident. However, a move to platforms that provide the same sort of convenience and functionality that consumers want, is evident from the increasing use of messaging apps. The theft of over 1 billion Indian citizen identities in 2018 demonstrated that WhatsApp was a platform that was capable of handling a massive sale of stolen identity data.

Overall, this means fraud detection and prevention (FDP) spend must be as broad as possible, as the potential attack vectors have massively increased. FDP vendors must be as actively engaged as possible in understanding new fraud methods to counter the high level of innovation in fraud methods.

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.

Investigation of darknet markets shows that neither expertise nor access to large sums of funding are required for fraudsters to gain a foothold in the market. The following tables give the average list price for various hacking tools, malware, templates and illicit guides on major darknet markets; a full kit of hacking tools can be purchased for around $125.

Table 1.2: Average Dark Market List Price ($), Various Tools & Products used by Fraudsters July 2018

Tools	Average Sale Price
Password Hacking Tool Custom Files	$1.96
Keylogger	$2.07
Phishing Page	$2.28
Wi-Fi Hacking Software	$3.00
Bluetooth Hacking Software	$3.48
FBI/NSA Hacking Tools	$5.64
Cryptocurrency Fraud Malware	$6.07
Hacking Software	$8.77
Remote Access Trojan	$9.74
Anonymity Tools	$13.19
Forgery Templates	$13.97
Carding Software	$44.37
Malware	$44.99
Password Hacking Software	$50.64
Cryptocurrency Miner Malware	$73.74
Fraudulent Account	$145.05
Cell Tower Simulator Kit	$28,333.33

Source: Top10vpn.com[viii]

Table 1.3: Average Dark Market List Price ($), Various Guides used by Fraudsters July 2018

Guides	Average Sale Price
Malware	$0.99
Phishing	$2.49
Postal System Stealth	$3.35
Account Hacking	$3.91
Wi-Fi Hacking	$6.35
Cashout	$7.76
Carding	$10.61
Security Bypass	$17.54
Dark Web	$31.20
Exploit	$2,536.56

Source: Top10vpn.com[ix]

b) Key Takeaways

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.

1.3.3 Identity Theft

Consumer-focused online transactions require consumer identity data to proceed. As the driving force for online transactions of all kinds, including payments, identity data is a prime target for fraudsters. In the US, the Consumer Sentinel Network, part of the Federal Trade Commission (FTC), tracks identity-related fraud. In their analysis of fraud types, in the year from Q3 2018 to Q3 2019, a 78.7% increase in credit card fraud was observed. There was a smaller increase of 11% in bank fraud in the same period. Other identity theft increased by almost 63%.

Figure 1.4: FTC Consumer Sentinel Network Snapshot 2019

Source: FTC

In the UK, Credit Industry Fraud Avoidance System (CIFAS) found an 8% rise in identity theft in 2018.[x] Similar patterns of identity theft occur throughout Europe.

- Online transactions increasingly require identity data to allow access to even the most ordinary resources. 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 (and hybrid on and offline) Know Your Customer (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.'[xi] This was echoed by research in Experian's "2018 Global Fraud and Identity Report" which demonstrated that 84% of businesses believe if they can solve the identity challenge, they can mitigate downstream fraud.

- 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, phishing being the top method to infect computers with malware according the Symantec's 2019 Internet Security Threat Report.[xii]

- Business Email Compromise (BEC)/CEO Fraud malware and possible augmentation using deepfakes continue to plague B2B wire transfers. According to Proofpoint, BEC campaigns in Q4 2018 had a y-o-y increase of 476%.[xiii] A recent BEC incident has been attributed to the use of deepfake technology. A British CEO transferred $240,000 at the request of the parent company CEO; the latter turned out to be a possible faked voice used during a call between the two CEOs.

- Deepfakes and identity is a concern for 77% of cybersecurity decision makers in the financial sector according to a report by iProov.[xiv] The report also found that around 50% of respondents believed deepfakes were a high risk for online payments.

- Synthetic Identity is where a cybercriminal uses snippets of legitimate data (like a Social Security Number) then add in other made-up data to create a synthetic identity. They then use this ID to commit fraud, including apply for loans, set up lines of credit, etc. A report by Aite Group found that US credit card accounts lost $820 million in 2018 because of SIF (Synthetic Identity Fraud).[xv]

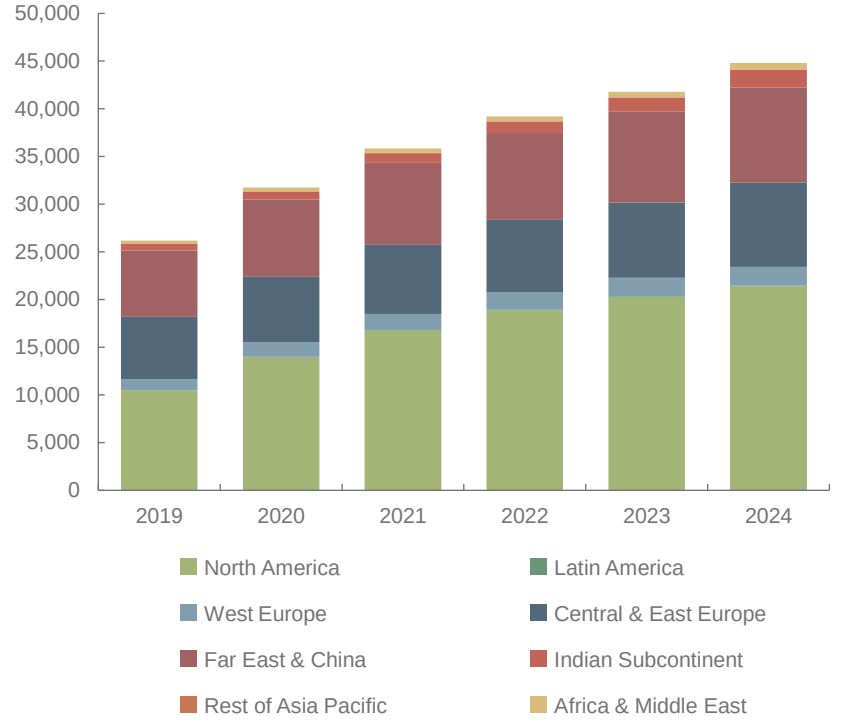
i. Data Breaches

Data breach volume and rates continue to rise, with a 54% increase in breached data records during the first half of 2019.[xvi] Juniper Research estimates that by 2024, cybersecurity breaches will result in costs of over $5 trillion. A substantial proportion of these breached data records contain sensitive personal or credential information that can be used in attempts to carry out fraud on a number of sites or services.

Data breaches are themselves a pathway to further crime. RSA has highlighted that mass data breaches are a means to enable account takeover.[xvii] Credential stuffing is one such follow-on activity; this is where previously exposed login credentials are used to facilitate account takeover. Akamai identified 61 billion credential stuffing attempts in the 18 month period to June 2019.

In order to circumvent the increased use of Multi-Factor Authentication (MFA) to protect account access, cybercriminals are using techniques such as channel jacking and SIM swapping to hijack bank and other financial accounts.

Figure 1.5: Total Number of Data Records per annum Exposed through Cybercrime (m), Split by 8 Key Regions 2019-2024



Source: Juniper Research

There appears to have been little let-up in the number and size of data breaches occurring y-o-y. There have already been a number of significant breaches in 2019, as shown in the following table:

Table 1.6: Selected Major Data Breaches Reported February-November 2019

Brand	Date	Impact
Verifications.io & MongoDB	Feb-19	763 million PII
Capital One	Mar-19	106 million including names, addresses, dates of birth, credit scores, Social Security numbers and bank account numbers
American Medical Collection Agency	Mar-19	20 million health data records
Canva	May-19	139 million PII and partial exposure of financial data
First American Financial Corp	May-18	885 million includes bank account numbers, mortgage details and other financial data
Desjardins	Jun-19	2.9 million PII, including banking habits
Suprema	Aug-19	27.8 million PII including biometric data
Unicredit Bank	Oct-18	3 million PII
T-Mobile	Nov-19	1 million PII

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. In 2019, misconfiguration and/or poor security measures were behind many of the largest data breaches. A cross-industry report from McAfee into Infrastructure as-a-Service risk found that '99% of misconfigurations go unnoticed by companies using IaaS'.[xviii]

This trend was corroborated by David Britton of Experian: 'Experian services many types of markets, including eCommerce, travel, and financial services, and we are seeing an increase in both new account fraud, as well as account takeover activity, via more creative cross-market attack vectors'.[1]

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. Digital identity is a key enabler in data theft and ultimately financial fraud. Payment service providers and merchants must continue to put robust structures in place to reduce the risk around the various types of identity fraud. FDP investments should focus on reducing synthetic identity and other misuse of identity accounts, including hijacking. The use of event-driven authentication and Anti-Money Laundering (AML) checks is another area to explore to prevent exploitation of existing relationships.

The FTC's annual report, the "Consumer Sentinel Network Data Book," highlights reported instances of identity theft of various types during 2018; key statistics from the report are tabulated right.

Relevant statistics here include bank identity fraud (up 14% y-o-y from 2016), as well as online shopping and payment account identity theft (up 43% y-o-y).

Table 1.7: FTC Reported Identity Theft Cases 2018 *vs* 2017

Identity Theft Class	Subclass	2018 Reports	2017 Reports	y-o-y Change (%)
Credit Card Fraud	New Accounts	130,928	105,209	24%
	Existing Accounts	32,329	34,260	-6%
Phone or Utilities Fraud	Mobile Telephone - New Accounts	33,466	26,062	28%
	Utilities - New Accounts	21,994	22,064	0%
	Landline Telephone - New Accounts	7,738	6,034	28%
	Mobile Telephone - Existing Accounts	4,983	4,675	6%
	Utilities - Existing Accounts	1,322	1,162	20%
	Landline Telephone - Existing Accounts	1,453	1,107	25%
Bank Fraud	Debit Cards, Electronic Funds Transfer, ACH	23,219	23,229	0%
	New Accounts	19,639	17,487	12%
	Existing Accounts	12,990	12,754	2%
Other Identity Theft	Online Shopping or Payment Account	10,294	8,685	18%
	Email or Social Media	9,439	7,645	23%
	Medical Services	13,833	6,805	103%
	Insurance	3,675	2,952	24%
	Securities Accounts	1,877	1,634	15%
Total		**329,179**	**281,764**	**17%**

Source: adapted from FTC Consumer Sentinel Data Book 2018

[1] Juniper Research Interview with David Britton, VP Industry Solutions Experian February 2020

ii. Cybercriminal Targeting Shifts

Analysis from cybersecurity firm Positive Technologies has shown that cybercrime attacks are more likely to be targeted ones, making up 59% of the attack total. Over half the attacks are focused on data theft, with 42% of attacks against individuals being financially motivated.

One interesting and pertinent finding from the report was that as financial cards and details are encrypted, cybercriminals are turning to more social engineering-facilitated attacks to elicit financial data and details.[xix]

A continued move by cybercriminals to reflect the omnichannel nature of the modern payment ecosystem is noted. Attacks are multi-faceted, 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.

David Britton from Experian commented: ‘Omnichannel is being challenged on a number of fronts; market conditions are driving the “always-on access” expected by the consumer. This requires ready access across traditional web, call-centre, chatbots and all other aligned channels. When organisations moved from web to app-based interactions, we saw some security issues coming into play, when banking went online, the individuals who developed the platform also had responsibility for security and risk management. When banking apps were required, they were often outsourced to get fast entry to market but in doing so, they lost the legacy of the rich risk management experience they had in the web development.’[2]

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:

- Identity data protection mechanisms across the board, including robust storage and access 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.
- Verification of an individual when creating an account tied to financial resources should include KYC and AML checks. Verification to a high level of confidence will require specialist third party identity and orchestration services.
- Robust authentication, including transaction authentication. Also, certain transaction checks could initiate a step-up of authentication, depending on risk-level.

[2] Juniper Research interviewed David Britton, VP Industry Solutions for Fraud & Identity Management, Experian, in February 2020

The use of point solutions to prevent payment fraud is like putting a sticking plaster onto a broken leg. Fraudsters are organised and collaborate to steal, share and utilise personal data, *en masse*. Payment fraud is a thriving business and like all good businesses, innovation leads to better products and more success. There is evidence of this not only in technological innovation but in the manipulation of human behaviour, otherwise known as social engineering. New technologies such as the AI-based deepfakes will take social engineering to unseen levels of success. As banking and online payments open their doors to digital assistant technology, it is highly likely the fraudster community will follow suit, perhaps integrating deepfakes with digital assistants.

In this highly integrated and complex web of payment fraud we have to look at all angles. Every aspect of security, from the shop floor personnel to the technical, must work together to create a holistic security machine. We must assume that a data breach is not *if* but *when*. A deeply layered and integrated approach to cybersecurity is required to tackle payment fraud. Payment Service Providers (PSPs) and merchants must consider fraud prevention and cybersecurity best practices under the same umbrella.

1.4 PSD2 Implementations & Future Challenges

1.4.1 PSD2 Overview

Payment Services Directive Two (PSD2), which was adopted by the European Parliament in October 2015, came into force in January 2018. The introduction of PSD2 means radical changes for the financial industry. The directive enables so-called Payment Initiation Service Providers (PISPs) managing payments in and out of an account and Account Information Service Providers (AISPs) 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 European Banking Authority (EBA) has been working with the European Commission (EC) on developing a so-called Regulatory Technical Standards (RTS) framework for Strong Customer Authentication (SCA), along with common and secure communications

1.4.2 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 Tink on the implementation of PSD2 by banks described the effort needed to get structure in place for compliance as 'monumental'.[xx]

The PSD2 Tracker report for April 2019,[xxi] found that 'only 25% of European online merchants are aware of the requirements under PSD2 for more robust and strong customer authentication'. By November 2019, the PSD2 report continued to find awareness issues amongst consumers and certain retail sectors. In the travel and hospitality sector, only 35% had reached compliance by the September deadline.

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

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;[xxii] 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.

1.4.3 RTS Implications for Payment Service Providers

i. Fraud Detection

Ongoing fraud detection for the entire payment lifecycle is strongly advised; from pre-authorisation through Pay Later schemes. Fraud detection is not a point action, it should be approached as a protective layer whenever a transaction occurs.

The ongoing protection of systems and services should include the detection of unusual patterns of behaviour. Advanced Persistent Threats (APTs) are designed for long-term exfiltration with stealth. Sophisticated methods of hiding APT malware will continue to create issues for easy detection of such malicious software using more traditional tools. Endpoint Detection & Response (EDR) tools can be a good holistic use of technology by alerting both the end-user and administration personnel to an imminent threat. Deception technologies are another useful area for trapping cybercriminals 'in the act'. However, 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. Traditional systems have utilised rules-based methodologies for detecting fraud, which can result in high numbers of false positives, requiring a high level of manual investigation and input. Modern approaches that leverage machine learning have shown a reduction in false positive results, as models 'learn' which results are actually fraud over time.

As channels of payment become multi-jurisdictional and cut across varying channels, risk profiles can be aggregated, providing a way to manage a complex payment ecosystems and security.

This whole world view of how payments work, from pre-authorisation and registration of a user through to transactions, is repeated across the industry. This reflects the highly connected, omnichannel nature of payments in the 2020s.

ii. 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 Risk-Based Authentication (RBA) 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:

    a) Abnormal spending patterns and previous transaction history;

    b) Software or device abnormalities;

    c) Malware infection;

    d) Fraud intelligence in respect to known activities or patterns;

    e) 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.

Table.1.8: 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

- Other exemptions apply, such as when the individual transaction value is equal to, or below, €30 ($34.80). Meanwhile, consumers will have the ability to nominate so-called 'trusted beneficiaries', where SCA will only be enforced during the process to enrol them.

- The entrance of child's cards, which are held by minors as beneficiaries, to the payments system must not be forgotten. Although spending limits can be placed on the card, the use of money mules in the younger age bracket is an increasing problem. UK consumer watchdog CIFAS, recorded 5,819 cases of money mules aged 14 to 18 years old in 2018. Younger children may be at more risk because of lack of security awareness.

a) Implications

During the lead-up to the finalised RTS, many stakeholders in the card payments industry voiced concerns about the strict enforcement of SCA, as ongoing security challenges would be inconvenient for the consumer, in turn driving increased demand for alternative payment solutions, such as bank transfers.

Following confirmation of SCA exemptions defined in the RTS, the incentive is quite clear: PSPs that are able to demonstrate a low fraud rate will be able to provide the most seamless experience for the consumer. This will inevitably result in both increased spending on FDP solutions in the EU, while also having implications on the FDP market itself:

- FDP solution providers which 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 is likely to take place to meet requirements for malware detection.

1.5 The API in the Machine

The ethos of Open Banking is gaining traction outside the EU. South Korea, Singapore and the US are major countries exploring the options offered by using this type of financial integration, with many cases involving private Open Banking schemes, rather than regulator-mandated rollouts.

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 Monetary Authority of Singapore (MAS).[xxiii] This initiative is helping to 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.

In Australia, Open Banking was stalled in late 2019 due to security concerns. A pilot program is planned to keep momentum on the project going. This will be performed by the Big Four Australian banks, alongside the Australian Competition and Consumer Commission (ACCC) and Data61. The program will enable more stringent testing of performance, reliability and security of the Open Banking services. The new date for delivery of the initiative is July 2020.[xxiv]

Delays are not uncommon, especially when highly innovative and interoperable systems are planned. The Tink survey found that 41% of banks missed the initial March 2019 deadline for setting up sandboxes for API testing, which is a crucial aspect of ensuring security is robust. A rush to integrate with Open Banking APIs and other ecosystem APIs should not compromise 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 cyber-attacks.'[xxv] As payment ecosystem players are often integrated via open API connections, this weakest link principle needs to encompass API security best practises. The EBA caveats this requirement with section 3.1 of the report by citing the 'proportionality principle'. Juniper Research recommends having robust vendor management that extends to API security; this is a must when utilising any API for added functionality in an extended ecosystem.

1.6 The Fintech in the Equation

Fintechs have taken the banking and financial sector by storm, innovating around initiatives such as Open Banking. They have also added new potential entry points for fraudsters into the payment ecosystem. Fintech offerings cover the gamut of consumer interactions with the payment ecosystem players. They are a major consideration in terms of payment fraud dynamics.

The resilience of fintech vendors has come under scrutiny. The European Parliament's 'on FinTech: the influence of technology on the future of the

financial sector' noted the risks linked to Fintech payment solutions, including 'fraud, misuse of consumers' data, weak authentication procedures.'[xxvi] The report recommends the use of standard APIs to encourage best practise security. Fintechs and any financial player adding a fintech solution to their ecosystem, should consider the enforcement of API standards and protocols. Fintechs endeavour to ensure a best-in-class approach to security to deliver a competitive edge. However, having a security policy that mandates a security-focused approach to the use of fintech solutions should be standard.

1.7 Consumer Behaviour, the Fraudsters' Friend

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 November PSD2 Tracker report noted that 32% of consumers would rather pull out of a purchase that goes through the extended authentication measures required by PSD2. A lack of awareness of the regulations and the reasoning behind more stringent authentication during a transaction also plays into the hands of the cybercriminal.

The report also found that there was a serious discrepancy between what retailers believed their customers understood about the needs for PSD2, and SCA in particular, and the reality of awareness.

A number of factors playing into the hands of cybercriminals. The success of social engineering in complex fraud such as BEC, along with more consumer-focused scams and phishing campaigns, has emboldened them. Efforts by the cybercriminal community to create 'as-a-service' cybercrime tools that begin with human intervention, has made the fraud industry highly accessible.

The connected payment universe, created by the advantages offered by an API economy, opens up new points of entry that allow cyber-attacks to propagate.

The mosaic implementation of SCA requirements for payment by varying retail sectors, coupled with a resistance from consumers to accept more stringent authentication, opens opportunities for cybercriminals to take advantage of social engineering.

i. 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 boon to 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 Financial Institutions (FIs) 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 OpenID Connect (OIDC) 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 session-less, 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 Open Authorization 2.0 (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 Open Banking Implementation Entity (OBIE) is attempting to standardise Open Banking in the UK, based on an enhanced version of OIDC. The result is an alignment between the OpenID Foundation (OIDF) and the Financial Grade API (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.

ii. 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.

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 eXtensible Markup Language (XML) and JSON 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 call and metadata, while 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 Artificial Intelligence (AI) to analyse API behaviour and spot patterns and anomalies that predict a cyber-attack. However, as a caveat, algorithms may assume that API usage is consistent; this could potentially reduce the effectiveness of the security offering. However, it is worth exploring AI-driven API security in the future.

1.8 3-D Secure 2.0 (3DS 2.0) & Biometric Authorisation of Transactions

Juniper Research expect that biometric authentication will be used to secure $2.5 trillion worth of mobile payment transactions by 2024. However, whilst 90% of smartphones will be biometric-enabled, only 30% will use biometrics for transaction authorisation.

3DS 2.0 aims to address many of the shortcomings of version 1.x and, when implemented in key eCommerce markets such as the US, it should have a dramatic effect in terms of fraud rates.

In Denmark, for example, there is noted a zero-abandonment rate and no fraud since the implementation of 3DS for Dankort cards.[xxvii]

The body developing the new standard, EMVCo, first announced the availability of 3DS 2.0 in October 2016. It will undoubtedly take some time before merchant uptake of the standard is widespread, due to the preparation needed. For instance, there are significant regional differences in how 3DS challenges are implemented:

- In European markets, approximately 90% of 3DS-enabled payments do not require an authentication challenge. This is due to European merchants and issuers using their own risk-based solutions to determine if a challenge should be issued.

- In the US, this figure falls dramatically, given that many issuers implement a 100% challenge strategy. This ignores the potential for datapoints to assess risk and improve the consumer experience. The new standard focuses on adopting a risk-based strategy which should render 100% challenge rates obsolete where it is implemented.

There are two significant benefits expected from 3DS 2.0 implementation:

- Reduced consumer friction: Merchants have previously been reluctant to implement 3DS 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 One-Time Passwords (OTP) typically sent via SMS, KBA or Out-Of-Band (OOB) authentication, which may use biometric information or a separate authentication mechanism.
- Multi-channel implementation: The new 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.

1.8.1 Further 3DS Implications

The 3DS 2.0 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 General Data Protection Regulation (GDPR) is concerned. Indeed, the question here is about transparency; if consumers are unaware of the types of personally identifiable information (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 Access Control System (ACS), 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, 3DS 2.0 reduces some of the friction associated with the inclusion of PSD2, SCA, for online payments. This is evidenced by data from Visa, showing that 3DS 2.0 has reduced checkout times by 85% and cart abandonment by 70%.[xxviii]

1.8.2 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 2024 for various global regions to help mitigate those threats.

Certainly, intelligent, AI/machine learning-based FDP approaches will be part of the anti-fraud toolkit of payment focused cybercrime. However, these must cover the myriad of touchpoints for a complex matrix of customer interactions on payment services. This is being challenged by the addition of omnichannel payment delivery in multiple jurisdictions that is enhanced and extended by Open Banking APIs. This is all in an environment where social engineering is keenly used for cybercrime purposes. The result is a massive number of variables to contain, without impacting a seamless customer experience.

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 covering everything from the verification of a customer to authenticating and authorising a transaction, to securing data at all points in its lifecycle.

Social engineering is a spanner in the works. It needs to be controlled from the leading edge by putting highly robust KYC measures in place to help prevent synthetic identity threats. It also has to be shored up, post-KYC, by strong authentication and authorisation measures that are phishing-proofed.

To address the challenges of identity, the industry will need to start collaborating much more closely with the government, to ensure high security standards and be able to identify the person as part of the KYC process.

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 Instead.

David Britton at Experian commented: ‘Online KYC and CIP are fundamental regulations that are a critical foundation, important because they require the business to perform due diligence during consumer engagement. While they are required to meet client’s needs, KYC alone is not enough to sort out the fraud problem. It is about having **layers of capabilities** that are needed to solve complex financial fraud. It is Experian’s strategy to bring together a number of native and partner capabilities via our CrossCore Platform to help solve these challenges.’[3]

Battening the hatches on 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 3.93%. Securing the system as a whole, for all the facets of modern digital payments, is the key challenge for 2024.

[3] Juniper Research Interview with David Britton, VP Industry Solutions Experian February 2020

2. Online Payment Fraud Competitive Analysis

2.1 Introduction

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

- Accertify (American Express)
- ACI Worldwide
- CyberSource (Visa)
- Experian
- FICO
- Fiserv
- Gemalto (Thales)
- iovation (TransUnion)
- Kount
- LexisNexis Risk Solutions
- NICE Actemize
- NuData (Mastercard)
- SAS
- Riskified
- RSA Security

2.2 Juniper Research Leaderboard

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

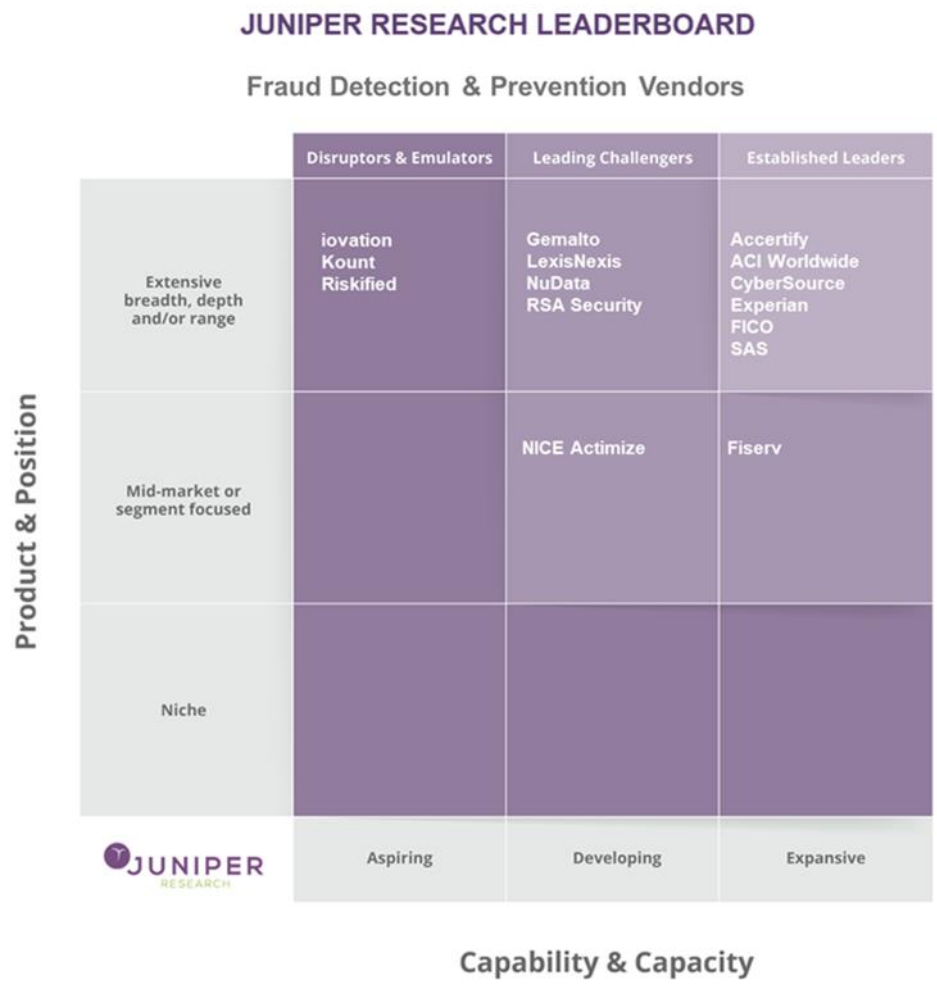
This technique, which applies quantitative scoring to qualitative information, enables us to assess each vendor's capability and capacity and its product and position in these markets. The resulting Leaderboard shows our view of relative vendor positioning.

Table 2.1: FDP Vendor Capability Assessment Criteria

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

Source: Juniper Research

Figure 2.2: Juniper Research Leaderboard: FDP Vendors



Source: Juniper Research

Experian continues to diversify beyond credit, with its standing heavily enhanced in the FDP market through its heavy investment in and increasing experience in machine learning. These expanded capabilities are available via the CrossCore platform which applies smart and flexible orchestration with powerful machine learning. It also has pre-configured integrations with a wide range of Experian and 3rd party capabilities including: identity verification solutions, device intelligence, Experian's FraudNet and Hunter's consortium and risk engines, document verification, and traditional and behavioural biometrics, making it a highly valuable FDP partner.

2.2.1 Limitations & Interpretations

Our assessment is based on a combination of quantitative measures where they are available (such as revenues 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 endeavours to provide accurate information; whilst information or comment is believed to be correct at the time of publication, Juniper 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 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: February 2020. It does not indicate how we expect positioning to change in the future or, indeed, in which direction we believe that the vendors are moving. We caution against companies taking any decisions based on this analysis: it is merely intended as an analytical summary by Juniper Research as an independent third party.

2.3 Experian Company Profile

Table 2.3: Juniper Research Leaderboard: FDP Vendors

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

HIGH LOW

Source: Juniper Research

Juniper Research interviewed David Britton, VP Industry Solutions, Fraud & ID Management at Experian, February 2020

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 revenues of $4.86 billion for the fiscal year ending in March 2019.

Key executives include Brian Cassin (CEO); Kerry Williams (COO); and 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; around 25% of revenues of the Decision Analytics division is attributed to identity checking and verification.

Table 2.4: Experian Financial Snapshot ($m) FY 2017-2019

	FY 2017	FY 2018	FY2019
Revenues	$4,335	$4,662	$4,861
Net Income	$865	$815	$701

Source: Experian

ii. Geographic Spread

Experian's headquarters are in Ireland. It has further offices in 44 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, NextCaller), email verification (Emailage), Alternative Data (Ekata, Global Data Consortium, HelloSoda, Pipl), Mobile Phone Verification (Boku/Danal) and Chargeback Management (Chargebacks911).
- Customers include banks, eCommerce merchants and retail companies, telecommunications providers, travel providers, health providers, insurance companies and public sector organisations.

iv. High-level View of Products

Experian's latest ID and Fraud flagship solution CrossCore, is an integrated digital identity and fraud risk platform that combines rich data assets from Experian with identity insights and capabilities from its curated partner ecosystem. Through sophisticated orchestration, it applies advanced analytics to give businesses confidence in every transaction. CrossCore combines risk-based authentication, identity proofing and fraud detection into a single cloud platform to make real-time risk decisions throughout the customer lifecycle. The platform is designed to help clients differentiate between their good and bad customers, without disrupting good customers, or increasing customer friction in their attempts to stop fraud. In order to address these challenges, the CrossCore platform provides:

- A single API with which clients can integrate any new or existing tools and systems all in one place, reducing complexity down into a single actionable decision.
- Self-service workflow orchestration and faster performance, which allows more client self-service control to easily implement strategy changes with no downtime to quickly respond to fraud threats while providing a safe and convenient experience for their customers.
- Partner integration: Experian's partnerships extend beyond technical integration, but include all contracting and due diligence with the vendor, such that the client only needs to amend their MSA with Experian to take advantage of the solutions
- Advanced 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.

Endnotes

i https://www.experian.co.uk/assets/business/reports/uk-i-identity-and-fraud-report-2019.pdf

ii https://www.experian.co.uk/assets/business/reports/uk-i-identity-and-fraud-report-2019.pdf

iii https://usa.visa.com/visa-everywhere/blog/bdp/2019/05/28/chip-technology-helps-1559068467332.html

iv https://www.proofpoint.com/uk/resources/threat-reports/human-factor

v https://terbiumlabs.com/resources/fraud-guides-101-dark-web-lessons-on-how-to-defraud-companies-and-exploit-data/

vi https://blog.cybersixgill.com/23million_stolen_cc_blog

vii https://www.rsa.com/content/dam/premium/en/white-paper/2018-current-state-of-cybercrime.pdf

viii https://www.top10vpn.com/assets/2018/07/Dark-Web-Market-Price-Index-Hacking-Tools-July-2018-Top10VPN.pdf

ix https://www.top10vpn.com/assets/2018/07/Dark-Web-Market-Price-Index-Hacking-Tools-July-2018-Top10VPN.pdf

x https://www.cifas.org.uk/insight/reports-trends/fraudscape-2019

xi https://www.finextra.com/videoarticle/2201/if-we-fix-digital-identity-we-fix-payments-tony-mclaughlin

xii https://www.symantec.com/security-center/threat-report

xiii https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

xiv www.iproov.com

xv https://legal.thomsonreuters.com/en/insights/articles/synthetic-identity-fraud

xvi https://www.riskbasedsecurity.com/2019/08/15/2019-on-track-for-another-worst-year-on-record/

[xvii] https://www.rsa.com/content/dam/premium/en/white-paper/2018-current-state-of-cybercrime.pdf

[xviii] https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/rp-cloud-adoption-risk-report-iaas.pdf

[xix] https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019-q2/#id3

[xx] https://tink.com/blog/2019/3/20/psd2-sandbox-status

[xxi] https://www.pymnts.com/tracker/psd2-april-2019-tracker/

[xxii] https://securityintelligence.com/news/phishing-attacks-exploit-new-online-security-checks-in-eu-uk/

[xxiii] https://www.mas.gov.sg/development/fintech/technologies---apis

[xxiv] https://www.openbankingexpo.com/news/australia-delays-open-banking-implementation-due-to-security-concerns/

[xxv] https://eba.europa.eu/sites/default/documents/files/documents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

[xxvi] http://www.europarl.europa.eu/doceo/document/A-8-2017-0176_EN.html

[xxvii] European Fraud Report: https://www.nets.eu/solutions/fraud-and-dispute-services/Documents/Nets-Fraud-Report-2019.pdf

[xxviii] Visa: https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-3d-secure-2-program-infographic.pdf