ONLINE PAYMENT FRAUD WHITEPAPER

2017-2022

Prepared for Experian

JUNIPER RESEARCH

First Published June 2017

Published by:
Juniper Research Limited,
Church Cottage House,
Church Square,
Basingstoke,
RG21 7QW, UK
UK: Tel +44 (0) 1256 830001/475656
US: Tel +1 408 716 5483
UK : Fax +44 (0) 1256 830093
www.juniperresearch.com
info@juniperresearch.com

Printed in United Kingdom

Report Author
Steffen Sorrell

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 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, Macedonia, Moldova, Montenegro, 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, 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, Swaziland, Syria, Tajikistan, Tanzania, Tunisia, Turkmenistan, Uganda, United Arab Emirates, Uzbekistan, Yemen, Zambia, Zimbabwe

Contents

1. Key Takeaways & Strategic Recommendations

1.1 Key Takeaways

1.1.1 Higher Walls lead to Higher Ladders

The recent move in the US to EMV cards using CHIP and signature technology has highlighted the fact that fraudsters do not give up when new walls preventing fraud are erected. Indeed, for fraudsters, this simply means building higher ladders.

In the context of the US, this has meant that CP (Card Present) fraud has now shifted online; higher levels of CNP (card not present) fraud have been observed, while synthetic account and account takeover fraud has increased dramatically.

1.1.2 The Internet of Things will Bring New Challenges

The IoT (Internet of Things) is rife with devices that have little, or poor, cybersecurity implementation. This has presented cybercriminals with swathes of new devices that can be hijacked and used for illegal purposes. For the time being, IoT botnets are used for DDoS (Distributed Denial of Service) attacks; however, this will undoubtedly expand to include IoT botnets to carry out automated fraud tasks. As botnets' sophistication increases, new defenses will be required.

1.1.3 Machine Learning & Biometrics will Prove to be Key Defense Weapons

Machine learning will undoubtedly play a role in the FDP (Fraud Detection & Prevention) ecosystem and its importance is likely to increase rapidly.

The reasons for this are twofold; traditional anti-malware tools are no longer able to keep up with the pace of evolving malware. Meanwhile, pure rules-based fraud prevention solutions can be 'gamed' by fraudsters. Introducing machine learning to help malware or fraud detection provides the opportunity to develop risk-based systems that minimize human intervention, while machine learning is adept at detecting subtle patterns that may normally be missed by humans.

1.1.4 The PSD2 will Have a Significant Impact

The PSD2 (revised payment services directive), due to be enforced in EU countries from 2018, will have a wide-ranging impact. In the first instance, it will demand 'strong customer authentication', which will encourage further take-up of fraud prevention software and services.

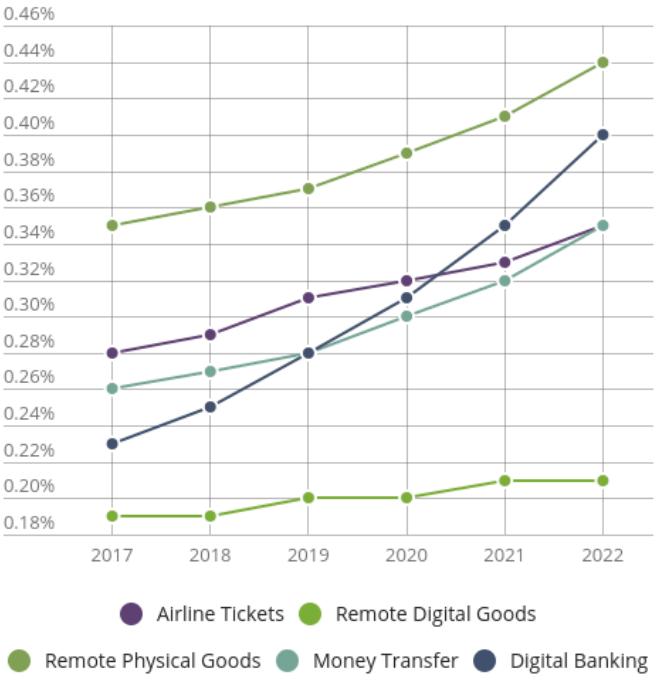
Meanwhile, the PSD2's aim to open up the payments space, leading to open banking APIs (Application Programming Interfaces) will offer new attack vectors for fraudsters. These APIs are likely to emerge not only in Europe, but also in North America and Asia in the near-term.

1.1.5 3DS 2.0 Delay Leaves a Fraud Window Open

3DS 2.0 (3D-Secure 2.0) has been touted as an important tool in addressing CNP fraud, with the ability to address online and mobile channels. Meanwhile, the level of data shared between merchants and issuers at the point of transaction will be unprecedented. Nevertheless, it will be approximately 2 years before 3DS 2.0 begins seeing wide take-up, as issuers and merchants must first prepare for rollout. Therefore, fraudsters are likely to attempt to capitalise on this 2 year window, leading to an increase in fraud attacks.

Figure 1.1: Online Payment Fraud Market Snapshot: Key Figures & Fraud Rates (%), Split by Segment 2017-2022

Many merchants still perceive combatting fraud as too expensive. Nevertheless, Juniper's cost analysis of FDP (fraud detection and prevention) solutions found that in most instances, merchants would receive value from their investment.



$19.3 Billion

Transaction value of card-not-present fraud in 2022

$11.8 Billion

Transaction value of money transfer & digital banking fraud in 2022

13.7%

Annual average growth of online payment fraud transaction value

$50.9 Billion

Cumulative spend on fraud detection & prevention software between 2017 & 2022

Source: Juniper Research

1.2 Strategic Recommendations

1.2.1 Invest in Fraud Detection & Prevention Software

This may seem an obvious solution, yet many merchants continue to perceive fraud prevention as too expensive, preferring instead to shoulder the cost of stolen goods or services. Juniper has found that in many cases, a ROI (Return on Investment) will quickly be realised even if the number of annual transactions is relatively low. Much of the cost of dealing with fraud is created through manual reviews, false declines and chargeback costs; a robust fraud detection solution will help avoid many of these costs.

1.2.2 Banks & Operators Should Collaborate Closely

Juniper has identified a rising trend in SIM swap fraud, which enables fraudsters to access end-users' bank accounts. With the fraudsters taking advantage of vulnerabilities across operators' and banks' processes, the 2 actors should collaborate in sharing historical customer data to help prevent this type of fraud.

1.2.3 Layered Approaches are Essential to Fraud Prevention

It is clear that fraudsters are adept at finding ways around the defenses built up in an attempt to stop them. Indeed, encountering barriers, fraudsters will rarely give up; instead, they will look for alternative openings. For this reason, a FDP solution must consist of multiple layers of protection; customers and service providers should assume that fraudsters will be able to penetrate at least one of those layers.

1.2.4 Fraud Prevention Service Providers should Work Closely with New Payment Service Providers

The emergence of open banking APIs will undoubtedly increase the scope for online fraud. Indeed, APIs are inherently vulnerable to exploits and often receive poor support. This means that fraud prevention services will likely be in high demand as these APIs emerge and are developed, leading to new opportunities.

1.2.5 Monitor the Session, not Just the Logon

Juniper has found that service providers often implement strong controls to prevent fraudsters accessing others' accounts. Nevertheless, once the logon has been authenticated, the assumption is that the user is genuine, thus leading to lax policies thereafter.

With fraudster tactics evolving to only enter the session after the genuine user has logged on, it should be essential that the whole session is monitored for fraudulent behavior, with checks applied as appropriate.

2. Online Payment Fraud Dynamics

2.1 Types of Fraud

There are numerous types of fraud and new opportunities for fraud arise as technology becomes more sophisticated and accessible. The following is a list of the top fraud attack methods, in descending order of prevalence:

- Clean Fraud – is a transaction that passes a merchant's typical checks and appears to be legitimate, yet 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 to combat clean fraud 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, in that a chargeback request is made in spite of received goods and services. While friendly fraud is non-malicious in nature, chargeback fraud occurs following a pre-meditated intention to commit fraud.

- Identity Fraud – is the fraudulent acquisition and use of sensitive personal information, such as national identification numbers (eg social security numbers), passports and driver's licenses. This information enables a skilled thief to assume an individual's identity and conduct numerous crimes.

- Affiliate Fraud – this type of fraud involves the fraudulent use of a company's lead or referral programmes to make a profit. For example companies may submit phoney leads with real customer information, or inflate web traffic to increase their payout before the merchant is aware of the scam.

- Re-shipping – this typically involves fraudsters recruiting an innocent person (known as a 'mule') to package and re-ship merchandise purchased with stolen credit cards. Since the mule has a legitimate shipping address, the merchant would have no reason to suspect fraud. The fraudsters then ask the unsuspecting individual to re-package and send the goods to them.

- Botnets – a botnet is a network of infected machines controlled by a fraudster (the 'botmaster') to perpetuate a host of crimes. In the case of eCommerce the infected device could be used with stolen payment and identity information, so the transaction appears to originate from a location that reasonably matches the credit card in use. In this way, infected computers appear to be 'good', when in fact they are not.

- Phishing – is the practice of sending seemingly official emails from legitimate businesses to steal sensitive personal information from customers, such as account log-in 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.

- 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 originated from within the targeted entity's organization, sent by another staff member, known business partner or other trusted party

- 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.

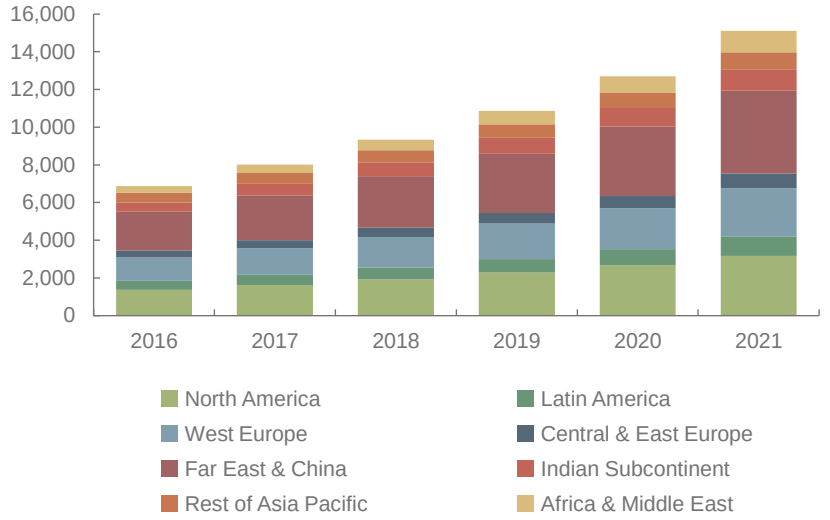
The only way to counter the fraud threat is through effective fraud management, consistently monitoring and updating fraud prevention configurations as fraud schemes change.

2.2 The Impact of the Internet of Things

Players across many industry verticals in the consumer segment have, over the last 3-4 years, caught on to the growing trend for the IoT. Unfortunately, this has resulted in an extraordinary number of connected units that have either poor, or no, measures in place to prevent unauthorized device access. The primary reason behind this disturbing trend is the fact that many consumer devices are very low margin products. Meanwhile, they are mostly sold on a transactional basis, meaning that revenues are only generated at the point of sale.

Cybersecurity is thus an afterthought, with devices being shipped with default credentials enabled, while the expense of patching any software vulnerabilities (alongside the complexity of doing so via white label products) means that many products fail to receive any critical security updates.

Figure 2.1: Consumer IoT Units (m), Split by 8 Key Regions 2016-2021



Source: Juniper Research

Botnets, or networks of so-called 'zombie' computers, have been in existence for some time, with miscreants often taking advantage of the ease of spreading malware via Windows PCs. Nevertheless, such botnets were restricted to home or enterprise PCs. Clearly, this situation has now evolved to the point where any hijacked IoT unit can feasibly be weaponized for the purposes of automated fraud workloads and other tasks aimed at facilitating fraud. While modern uses for botnets typically involve attempts to spread malware or to engage in DDoS (Distributed Denial-of-Service) attacks, Juniper believes that the following will only increase as both the IoT expands and as 'Malware as a Service' and 'Fraud as a Service' proliferate on the Dark Web.

2.3 Evolution of Fraudster Attacks – Key Takeaways & Recommendations

Service providers must be mindful of the evolving way in which fraudsters attempt to either gain access to end-user accounts, or to commit identify fraud.

2.3.1 'Sleeper' Attacks

Discussions with interviewees highlighted that while malware used to access user accounts is as prevalent as ever, the methods by which fraudsters are evading detection are changing. Christopher Schenking at Gemalto explained: 'Things like RATs (remote access Trojans) and things along those lines are being used differently. A lot of players in banking, in the CNP space, place a lot of emphasis on the first interaction. So a lot of checks happen there, creating a strong front door. But once those are verified, then the checks by and large stop, or are quite weak in detecting anomalous activity. So RATs are now being used by fraudsters to allow the user to log in and then jump in later during the session.'[1]

Indeed, it was noted that most service provider checks took place during the initial customer authentication stage, such as during login. Thereafter, it would be assumed that the user is genuine, with few active anti-fraud checks in place to prevent unauthorized transactions. In response to this strategy, fraudsters are increasingly employing a 'sleeper' tactic, whereby no criminal action is taken until after the login process. After the genuine user is logged in and fraud defenses are reduced, the malware is used to perpetrate fraudulent transactions.

Juniper therefore recommends that user behavior is constantly monitored in an attempt to separate genuine users from fraudsters. Meanwhile, MFA (Multi-Factor Authentication) challenges for high-risk transactions should be implanted as standard.

'There are elements that are gathered at each stage of the customer experience. The fraud systems that are the most effective are the ones that are able to find inconsistencies at each snapshot in time. You have to be able to string those pieces together to build a comprehensive overview of the session and an effective defense.' CyberSource[2]

2.3.2 Mobile Bots

Through a combination of poor service from device OEMs (Original Equipment Manufacturers) and network operators, many mobile devices are vulnerable to malware, which consequently can be used to turn devices into bots. These are then used to attempt carding or card cracking attacks.

[1] Juniper Research interviewed Christopher Shenking, Digital Banking Solution Manager, Risk & Fraud, Gemalto, June 2017

[2] Juniper Research interviewed a CyberSource representative, June 2017

In an effort to reduce costs, fraudsters will often use a single mobile device to register several payment cards at once. In turn, this increases the velocity of transaction attempts. As a result, monitoring of transaction velocity is an essential part of any anti-fraud solution.

Mike Lynch from InAuth noted: 'The next generation of bot-prevention tools involve device intelligence, device fingerprinting, malware detection, machine learning and behavioral analysis. This model relies more on identifying the bot at the root, that is, at the device level. Doing so makes it easier to employ both static techniques, such as detecting the presence of malware on the device, and a more complete behavioral analysis. That is, detecting a high number of attempts, a high number of failures, unusual traffic patterns, unusual speed of access and access attempts; that is more accurate and not so easily fooled.'[3]

[3] Juniper Research interviewed Mike Lynch, Chief Strategy Office, InAuth, June 2017

Case Study

i. Case Study: InAuth

InAuth

InAuth, acquired by American Express in December 2016, has adopted a mobile-first approach to its anti-fraud solutions.

The company is able to authenticate devices via its InPermID which the company claims cannot be spoofed and is able to survive system upgrades and uninstalls. In this manner, InAuth is able to leverage the past history of the device itself as a tool to prevent fraud.

Meanwhile, InAuth sees app tampering as a growing issue. The company offers service providers the ability to validate end-users' apps against their own to reduce instance of fraud conducted using bogus apps.

2.3.3 App Tampering

Juniper has found that as digital commerce moves increasingly to the mobile environment, fraudsters are attempting to manipulate the apps available to gather confidential account and consumer information for future account takeover or fraud.

2.3.4 Account Takeover & Synthetic Account Fraud

Several of our interviewees have noted an increase in instances of account takeover and synthetic account fraud, whereby automated scripts are used either to compromise existing accounts, or create new synthetic identities. Indeed, analysis by DataVisor in 2016 highlighted that a large retailer was targeted by login attempts from thousands of IP addresses in a single day. Each login attempt was conducted using a different browser cookie, defeating one of the device tracking mechanisms used in anti-fraud solutions.

'One of the big changes has been the rollout of EMV in the US specifically, which has led to a dramatic increase in the amount of account origination fraud, alongside account takeover fraud.' David Britton, Experian[4]

Where new accounts are created, or existing accounts are compromised, typically the bulk of the victim's information will be retained to evade detection. Meanwhile, a small number of attributes, such as mobile number or email address may be changed. Having achieved this, fraudsters will typically execute a number of legitimate transactions (which will be invisible to the victim owing to altered contact details) to build up a 'good' reputation with the merchant or service provider. Once this reputation is established, the fraudsters will then strike by executing a high-value transaction, with the assumption that the reputation with the merchant will lead to the transaction being viewed as low-risk and thus not subject to stringent anti-fraud controls.

Without a multi-layered approach to fraud detection, this type of fraud is difficult to fend off. Juniper believes that the key to controlling this activity lies both in the detection of 'abnormal' behavior and in the ability of service providers to collaborate and share datapoints with regard to known suspect IP addresses and contact details. Certainly, logs detailing normal login behavior for IP addresses, device type and time of day will provide a useful set of information that fraudsters will struggle to replicate. MFA should be used as additional protection from changing any details on the account meanwhile. Synthetic account creation is yet more difficult to combat compared to compromised account details and should rely on IP and device fingerprint blacklists to root out suspicious actors.

'The most important tools right now are automation detection and RAT (remote access Trojan) detection' Alexander Ermakovich, Kaspersky Lab[5]

2.4 FDP Service Provider Evolution

The following section will examine how FDP service providers are evolving their solutions in reaction to increased fraudster sophistication.

2.4.1 3D Secure 2.0

The version of 3DS currently in most widespread use (1.0.2) suffers from drawbacks that discourage both consumer use and merchant integration:

- Poor mobile integration;
- Potential for MITM (man-in-the-middle) attacks;
- Being mistaken as a phishing scam by the end-user;
- End-users have to enrol in the service with their bank before benefiting;

[4] Juniper Research interviewed David Britton, VP Industry Solutions, Fraud & ID Group, Experian, June 2017
[5] Juniper Research interviewed Alexander Ermakovich, Head of Fraud Prevention, Kaspersky Lab, May 2017

- The challenge method (password) means that the system is only as strong (or weak) as the password chosen by the end-user. There are no standardized requirements regarding password strength, leading to passwords that can potentially be broken by brute-force.

These factors have led to increased instances in cart abandonment where 3DS is integrated into the checkout flow which, in turn, has discouraged wider uptake by many merchants. The reduction in instances of fraudulent transactions is undeniable; however, merchants have felt that in some cases the potential revenue lost through cart abandonment is greater than the potential loss through fraud.

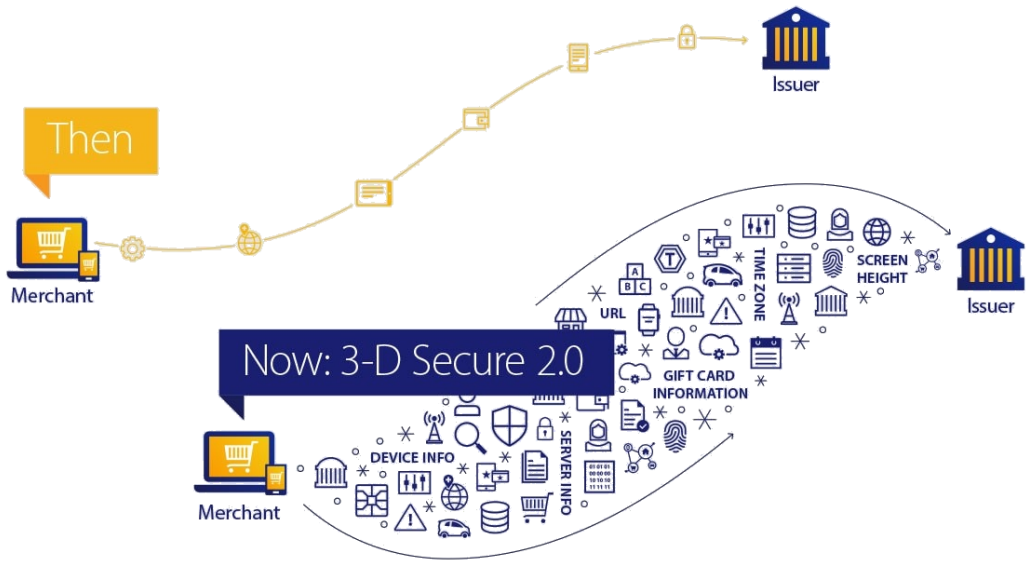
The industry has reacted to these shortcomings with the development of 3DS 2.0. This version aims to address many of the shortcomings seen in version 1.x while, importantly, version 2.0 will aim to be compatible with the demands set out in the PSD2.

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, owing 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:

Figure 2.2: 3DS1.x vs 2.0



Source: Visa

The introduction of this feature into the standard will mean that issuers such as Visa and Mastercard will incorporate more cardholder data into the model. Meanwhile other information, such as the device being used, time zone and so on, will help determine whether the buyer is genuine or not. Indeed, the ability for merchants to combine their own customer data (reputation, behavioral indicators and so on) with issuer data is a paradigm shift compared to how the standard was managed before. This should dramatically improve the service in terms of its risk-based approach.

In many instances, particularly where mid- to high-end mobile devices are used, biometrics may be used to authenticate the user, while the aim is to replace static passwords prevalent in version 1.x with OTPs (One Time Passwords).

One of the key factors in determining the spread of 3DS 2.0 will be in how quickly issuers respond to the new feature set. Version 2.0 for example, is not backwards compatible with earlier versions, which will mean that MPI (Merchant Plug-In) providers send the correct messages to the issuer depending on the latter's capabilities. Indeed according to CyberSource, even in a mature eCommerce space such as EMEA, only 80% of issuing banks had adopted a risk-based approach in 2014.[i] This proportion has undoubtedly increased since then, particularly as machine learning solutions have been democratized over the last 3 years. Nevertheless, other regions will have a significantly lower proportion of issuers able to adopt a risk-based approach. In effect, this means that adoption in emerging eCommerce markets is likely to be lower. In such markets the mobile device often is the primary computing device, so will be more likely to suffer fraud owing to no, or poor, implementation of the old 3DS standard.

Meanwhile, there are several operational changes that must occur at various nodes in the payment channel for 3DS 2.0 to be supported:

- Payment technology providers, payment processors and gateways must work with the new specification and accompanying SDK (Software Development Kit). EMVCo has made the specification for browser and mobile app-based authentication available for download free of charge, however;
- A framework for functional testing and compatibility with the new specification is still under development, with additional work by the PCI (Payment Card Industry) Security Standards Council for data security requirements, testing procedures, assessor training and reporting templates to address environmental security to be completed. EMVCo expects these documents to be released during 2017;
- Merchants and issuers will need to update their internal systems to ensure that they are ready for the new standard. This will require work by MPI providers as well as the third party ACS (Access Control Server) providers commonly used by issuers.

In conclusion, it will be some time before the new standard will be rolled out and in widespread use, given that full work on the developer side is unlikely to begin before the latter end of this year. Indeed, Visa estimates that rules for merchant-attempted 3DS transactions will extend to 3DS 2.0 from April 2019.[ii]

i. PSD2

Juniper believes that the PSD2 will have a significant impact on the speed of 3DS 2.0 rollouts within the EU. On account of its static password scheme, the current version of the standard does not comply with PSD2

demands for SCA (Strong Customer Authentication). However, the latest version, through adoption of biometrics, tokenisation and OTPs will meet the PSD2 requirements and can thus be used as part of the MFA challenge flow. It is therefore likely that EU countries will lead both in development and rollout of 3DS 2.0.

2.4.2 Machine Learning

A key factor impacting not only the financial industry but also several other market verticals, is the democratization of machine learning. So-called 'deep learning' algorithms (multi-layered artificial neural networks) and others not only require significant computing power, but also large volumes of data to be 'trained' to perform effectively. This has meant that, in the past, machine learning was confined to academia or high-revenue institutions able to fund high-performance computing, as well as acquire large amounts of useful data.

The advent of cloud computing, Big Data and the mobile device have effectively eradicated these issues, with frameworks for algorithms readily available, as well as being accessible to use via cloud computing services. Meanwhile, the financial industry can be viewed as one of the early pioneers of so-called expert systems driven by neural networks used to detect fraud, so the transition to modern machine learning is not an unfamiliar one for many players.

'The greatest purpose of machine learning is to augment traditional rules-based systems. It adds data and insight from a whole world of transactions, giving a broad view that can be used in fraud prevention.'
Dwayne Melancon, iovation[6]

i. Drivers

Many existing FDP solutions rely on rules-based systems in an attempt to root out fraudsters. While these are certainly effective at first, rules systems tend to be relatively static and are thus susceptible to gaming by fraudsters; rules are tested and then circumvented. Naturally, this results in a reaction by the service provider, who alters the ruleset. In turn, this results in a game of cat-and-mouse between fraudsters and service providers, effectively increasing the cost of combating fraud.

'We see more merchants looking to understand a customer's typical shopping and payment patterns to help assess the risk of a transaction. For example, someone who has purchased a last-minute, first-class business ticket to London previously without a chargeback may be scored differently than a person who has never exhibited this behavior before.' Lisa Rankin, Accertify[7]

[6] Juniper Research interviewed Dwayne Melancon,, VP of Product, iovation, May 2017
[7] Juniper Research interviewed Lisa Rankin, Vice President - Partnerships, Marketing and Sales, Accertify, June 2017

The benefits of using machine learning models to determine a transaction in terms of its risk are numerous:

- An ability to leverage a complex relationship between multiple data inputs rather than a rigid rule structure;
- The model is able to evolve over time and improve as more data is input and patterns are understood;
- New trends in fraudster approaches can be added to the model to react to prevailing market conditions;
- Models are able to use behavioral inputs, such as mouse movement, touch screen behavior and various other indicators to separate genuine user behavior from fraudulent behavior.
- Algorithms are able to detect patterns in data that would normally be hidden, thus offering the potential to save human-hours.

ii. Components

Development of FDP solutions using machine learning-based detection requires considerable effort and expertize. In the first instance, one cannot hope to develop a successful detection system without a historical dataset, ideally with at least a year's worth of data for training. In turn, this means that development of a machine learning anti-fraud solution requires expertize in terms of sourcing a high-quality dataset as well as in being able to determine that algorithms are optimized.

In short, planning for a machine learning-based solution will take at least one year. After deployment, it is often said that algorithms monitoring behavioral aspects on sites and apps take roughly 90 days to 'learn'. Nevertheless, some companies, such as Mastercard subsidiary NuData, claim that this can be reduced to 30 days.[8]

Once an effective algorithm has been developed, a platform will be required to deploy the solution to perform real-time scoring on transaction requests or account management.

Given the level of expertize required to develop and integrate a machine learning solution as a risk-based anti-fraud solution, most commonly a third party solution will be sought.

2.4.3 Layered Approaches

Although machine learning is being touted as the 'next big thing' in FDP solutions, and in the financial industry in general, it is important to acknowledge that a layered approach is far more effective than relying on a single defense strategy.

Whilst different vendors may offer different combinations of layers (and terminology), the most significant layers typically included in a FDP solution are as follows:

- **Layer 1: Endpoint-controls** – involves analysing user devices (PCs, laptops, mobile/fixed phones) for identity, location and authentication data.

  The very minimum standard for low-risk scenarios is 2FA (2-Factor Authentication), which might consist of a combination of software or hardware ID and a PIN or a user ID and a password. For higher-risk

[8] Juniper Research interviewed Robert Capps, VP of Business Development for NuData Security, May 2017

scenarios, a 3 factor authentication is more secure but is also more inconvenient.

For defense against MITM attacks OOB (out-of-band) authentication is used which requires separate information channels for authentication and access.

- **Layer 2: End-user browsing behavior** – compares website behavior with what is expected. Layer 2 controls include real-time, dynamic capture of customer and account online activity, which is used to build a customer profile to determine what is normal or abnormal for this customer.

Layer 3: Transaction monitoring by channel – this layer provides transaction analyzes of users and accounts by channel, for example, online, mobile, ACH (Automated Clearing House), ATM, etc and compares this activity to the normal for that user in a specific channel.

- **Layer 4: Cross-channel, cross-product transaction monitoring** – this involves taking a cross-channel approach to scoring transactions across multiple channels and products. Transactions that initially look innocent may appear suspicious when correlated with activities in other areas.

- **Layer 5: Holistic analysis** – Layer 5 controls go beyond transaction and customer views to analyze activities and relationships within a network of related entities.

FDP solutions use entity link analysis to discover potential relationships between devices, users, accounts and other entities, and can identify patterns of behavior that only appear suspicious when viewed across these related entities. It is thus possible to discover whether an identified suspicious behavior is limited to an isolated individual or is part of a criminal conspiracy.

Most financial services companies have implemented some form of controls at Layers 1-3. However, Layers 4 and 5 are the silver and gold standards in the industry at the moment, which only a few companies have reached.

3. FDP Vendor Analysis

3.1 Introduction

Given the breadth of vendors involved in the FDP landscape, this section will look at a select profile of the vendors 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.

- Experian
- Accertify (American Express)
- ACI Worldwide
- CyberSource (Visa)
- iovation
- FICO
- Fiserv
- Gemalto
- NuData (Mastercard)
- ThreatMetrix
- RSA

3.2 Juniper Leaderboard

Our approach is to use a standard template to summarize 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. Readers should note that criteria for assessing positioning within the Juniper Leaderboard are markedly different from those for its predecessor, the Vendor Matrix, and thus positioning within the former cannot be compared directly with positioning within the latter.

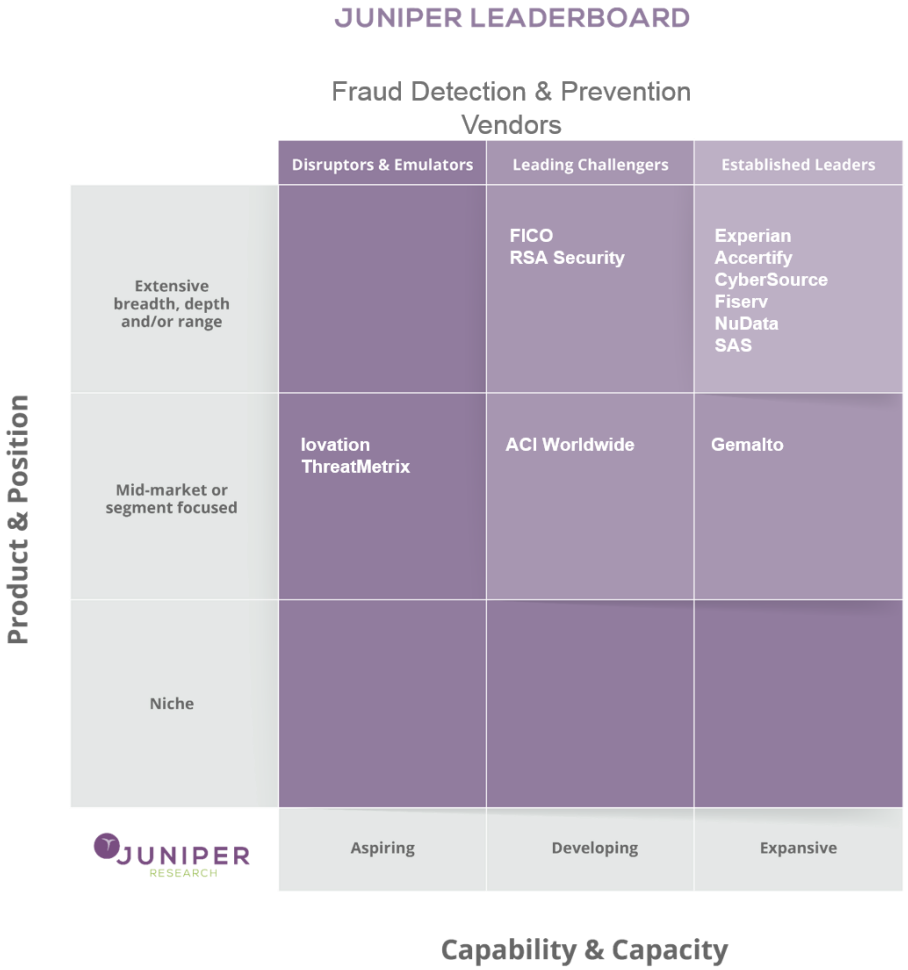
We have assessed each vendor's capabilities against the following criteria:

Table 3.1: FDP Vendor Capability Assessment Criteria

Category	Criteria	Description
Capability & Capacity	Financial Performance in Sector	In assessing this factor we considered the FDP performance of the vendor 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 their experience are taken into account here.
	Operations & Global Reach	This factor considers primarily the overall extent of geographical penetration of the vendor 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 Value Added Retailers.
	R&D Spend	An indicator of the investment a vendor is making to develop best-in-class solutions; Mergers & Acquisitions 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 their 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 within the segment, with a view to augmenting their FDP capabilities.
	Creativity & Innovation	This factor assesses the vendor's perceived innovation through its flow of new features, products, developments and enhancements.
	Future Business Prospects	This factor relates to the ability of the business to develop and compete against others in the future.

Source: Juniper Research

Figure 3.2: Juniper Leaderboard: FDP Vendors



Experian is able to draw on a long history of measuring risk coupled with a robust FDP solution, bolstered by the acquisition of 41st Parameter.

Source: Juniper Research

3.2.1 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'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 fulfiling 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: June 2017. 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 as an independent third party.

3.3 Company Profiles

3.3.1 Experian

We have mapped out the results of our assessment, displaying 12 stakeholders on the Leaderboard.

Table 3.3: Juniper Leaderboard: FDP Vendors

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

HIGH ●●●●●● LOW

Juniper Research interviewed Eric Kingsbury, Senior Manager, Product Marketing, John Sarreal, Product Manager, Fraud & ID Group and David Britton, VP Industry Solutions, Fraud & ID Group at Experian, June 2017

i. Corporate Profile

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. It had revenues of $4.3 billion for the fiscal year ended in March 2017. Key executives at the company include Brian Cassin (CEO), Lloyd Pitchford (CFO) and Barry Libenson (CIO).

Perhaps best known as one of the biggest credit reporting agencies, the company's main business divisions include Credit Services, Decision Analytics, Marketing Services and Consumer Services.

The company's fraud solutions are reported under its Decision Analytics segment. Evidence from its annual financial reporting suggests that the company's FDP offering is relatively stable.

The company has a long tradition in providing identity proofing services and around 80-90% of revenues of the Decision Analytics division is concerned with identity checking and verification.

Table 3.4: Experian Financial Snapshot ($m) 2015-2017

	2015	2016	2017
Revenues	$4,810	$4,237	$4,335
Net Income	$1,006	$966	$1,071
Decision Analytics Revenue Share (%)	12.3%	12.4%	13.5%

Source: Experian

In April 2014, Experian acquired 41st Parameter for $324 million, a provider of device identification technology for web fraud detection, to strengthen its web fraud detection and 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 located in Ireland. It has further offices in 37 countries across the globe in 6 continents.

iii. Key Clients & Strategic Partnerships

- Experian has a wide range of partners, some of which are not publicly disclosed. Key publicly announced partnerships include ACI WorldWide, FICO, NuData Security, BioCatch, Symantec and WhitePages Pro. Mobile payments company ACI, for instance, has an agreement with Experian to market its analytics-driven decision solutions to ACI's customers and prospects.
- The company partners with leading technology partners, for example, to create IP geolocation data.
- Customers include banks, eCommerce merchants and retail companies, telecommunications providers, travel providers, health providers, insurance companies and public sector organizations.

iv. High-level View of Products

Experian offers a range of fraud and authentication products which draw in large sets of data about people and devices to recognise customers and detect fraud.

In June 2016, Experian launched their flagship CrossCore fraud platform. The platform has been promoted a 'smart plug-and-play platform', given its ability for customers to connect their own solutions, Experian products and third party vendor solutions. This enables a highly-integrated approach to fraud detection and management, and allows customers to respond rapidly to changing requirements and industry trends. The platform's key features include:

- A flexible API that allows businesses to use and apply a range of identity and fraud tools from Experian, partners and the client's own internal

analytics in decisions to improve risk controls while reducing integration cost and complexity;

- Strategy design and workflow decisioning functions enable fraud and compliance teams to apply services in any combination to get the level of confidence required;
- SaaS delivery model;
- Encompasses all of Experian's fraud products and partner tools.

Another of Experian's offerings in the online payment fraud space is FraudNet, which is based on technology developed by 41st Parameter. Customized versions of the FraudNet platform have been developed to suit specific verticals such as:

- FraudNet for eCommerce
- FraudNet for Travel (ideally suited to the airline business)
- FraudNet for Banking

The FraudNet platform uses a highly configurable rules-based engine that analyzes transactions and is designed to balance business needs with fraud-risk appetite. The core FraudNet platform contains a number of solutions which can be configured according to the customer's requirements:

- FraudNet for Account Opening – a solution that helps in opening and determining the level of risk in establishing a new account.
- FraudNet for Account Takeover – a fraud management application that covers account takeover activities.
- FraudNet for Transactions - a rules-based risk engine that analyzes transactions to determine the level of risk.

In July 2012, Experian launched PowerCurve, which became the core of its Decision Analytics platform. This unit provides credit and non-credit data, customer analytics and fraud detection to lenders, retailers and eCommerce firms, cable and satellite companies, telecoms firms, debt collectors, utilities and state and federal government entities.

Future strategies for the company include mitigating the threat posed by the IoT and the potential for fraud raised by these devices. 'A key area of focus for us has been, "what is identity?", asking if we can get beyond a single individual and understand their network of devices, who their proxies are and what their devices are? In that way we can create profiles that include the various devices and agents that are connected to an entity,' explained Eric Kingsbury.

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

- The company's new CrossCore platform allows customers to easily deploy best-in-class solutions across a range of vendors. Costs and complexity are thus reduced.
- Experian believes that its fraud detection rates are better than any of its competitors. The company defines the accuracy of its fraud detection as the percentage of fraudulent attempts (losses plus stopped fraud attempts).
- Experian claims that it shows its customers between 2-5% of their traffic total are fraudulent transactions, which includes the rejected and the manual review rate. The industry average for other vendors in this space

is as high as 25% held for manual review and an additional 7% being rejected.

- Experian claims that the patented device intelligence solution developed by 41st Parameter is superior to competitors' solutions and is more effective in reducing false positives.
- Experian believes the reason for this effectiveness is the superiority of its rules-based risk engine, which uses advanced device intelligence to analyze the characteristics and configuration of devices used to make payments. The company believes that a rules-based risk engine is more accurate than a behavioral-based engine in a real-time fraud detection environment. However, the company does use behavioral analytics and Big Data offline.

Endnotes

[i] https://www.youtube.com/watch?v=1KXRti6oMcE

[ii] https://usa.visa.com/visa-everywhere/security/future-of-digital-payment-security.html