ONLINE PAYMENT FRAUD WHITEPAPER

2016-2020

JUNIPER RESEARCH

Contents

1. Online Payment Fraud: Key Takeaways & Strategic Recommendations

1.1 Key Takeaways

1.1.1 Online Fraud is Increasing & Spreading Globally

Online fraud is increasing and spreading rapidly across geographies and industries, despite merchants and FIs (financial institutions) investing more in fraud prevention. As soon as a new technology or process is deployed to prevent fraud, the fraudsters find a weakness to exploit or alternatively focus their attention elsewhere.

Key drivers behind the growth of fraud include the rapidly expanding eCommerce market, higher money flows in the online channel, and the increased use of mobile payments.

In general, the most common use cases are new account fraud (fueled by recent increases in data breaches), account takeover fraud and payments fraud (across all payment types and networks)

1.1.2 Introduction of EMV Results in a Spike in CNP Fraud

Although a problem for both CP (Card Present) and CNP (Card Not Present) transactions, card fraud is a bigger problem for online payments, i.e. eCommerce CNP transactions.

In many developed countries, CNP accounts for 60%-70% of all card fraud and is increasing.

History shows that the introduction of EMV in a country results in a significant drop in CP fraud, but a spike in CNP fraud.

Merchants and card issuers in the US should be prepared for an increase in CNP fraud as EMV migration takes place, although the rise may be more gradual than in other markets since there will inevitably be a lag in issuers and merchants upgrading their portfolios to chip-based cards.

Another factor could be the moderating impact of FDP (fraud detection & prevention) solutions, as merchants and issuers alike have been bolstering their CNP fraud detection capabilities significantly in recent years.

1.1.3 Mobile Payment Fraud is a Growing Problem

Mirroring the rapid increase in the popularity of mobile payments, it is evident that online fraud is expanding rapidly beyond traditional PCs to mobile and tablet devices, which is will likely to accelerate in the future.

Mobile devices face the same security risks as PCs and laptops, including viruses and other types of malware. Although the threat from mobile malware has increased significantly over the past few years, smartphone security does not yet match traditional computer security. For instance, security software is less common in smartphones, OSs (operating systems) are updated less frequently and mobile social networking applications sometimes lack detailed privacy safeguards.

1.1.4 Digital Security Vendors are Developing New Fraud Detection Tools & Authentication Techniques

Security vendors have responded to the increasing threat of online fraud by developing new fraud detection tools and advanced MFA (multi-factor authentication) techniques, involving OOB (Out-of-Band) authentication and using biometric technology for identity verification.

Biometrics is particularly applicable to smartphones, many of which are equipped with fingerprint, iris and facial recognition and can also analyse the phone user's voice. Several of the top FIs have already launched biometric-based identification and authentication solutions in their products.

1.1.5 Merchants & Financial Institutions are Being Driven to Invest in Increasingly Sophisticated Fraud Detection & Prevention Systems

A few years ago, in-house FDP solutions might have been adequate to keep fraud to acceptable levels. However, this is no longer the case. Fraudsters now operate globally and need to be dealt with by means of sophisticated, real-time fraud screening solutions, supported by an understanding of the latest fraud patterns and behaviours around the world.

Key attributes of these FDP solutions include:

- A multi-layer approach, typically 2 or 3 layers, which encompasses endpoint controls (analysing users/devices), end-user browsing behaviour (which compares user website behaviour with expected behaviour) and transaction monitoring. The rationale here is that if fraudulent activity is not detected by one layer, it will likely be picked up by another layer.
- The use of advanced data analytics, coupled with a holistic approach, which enables the analyses of fraud across several different channels simultaneously (eg online, ATM, call centre, etc) as fraudulent activity typically involves more than one type of mechanism or channel.

The FDP solutions vendor market is dominated by a few big, established players, including online payments processing companies such as ***ACI Worldwide, Visa*** and ***American Express***; information services companies such as ***Experian, FICO*** and ***SAS*** and digital security software companies such as ***RSA*** and ***Gemalto***.

These companies see FDP as complementary to their existing businesses and, in most cases, acquired their FDP capability rather than developing it in-house.

There is also a host of tech-start-ups which operate as niche players and offer limited FDP functionality. As an alternative to a full-blown FDP solution, some FIs prefer to rely on in-house solutions, using key technologies developed by the leading FDP tech start-ups to supplement these systems.

As a result, the tech start-ups are starting to compete effectively and are taking market share from their bigger brethren, some of which also use their technology.

1.2 Strategic Recommendations

1.2.1 Invest in Top-of the-Range FDP Solutions

The most appropriate type of FDP solution for a particular application or vertical depends on a number of factors. Some vendors develop solutions for individual verticals, such as the airline eTicketing market, or specific sectors of the financial industry, whereas others offer more general solutions that are suitable for all verticals and types of transactions.

An increasing number of solutions feature several 'layers' of protection, but the specifics and capabilities of each layer can vary significantly between providers. Real-time detection and interdiction capabilities are necessary to prevent online fraud.

However, not all FDP solutions currently offer real-time monitoring of all records, with some only analysing around 25% of all transactions. Another differentiating element is the data analytics (the secret ingredient of an FDP solution), as is the ability to offer cross-channel monitoring.

Leading FDP vendors operating in the airline industry report that they can reduce fraud levels typically to less than 0.1% of transaction values, with some claiming fraud levels of 0.01% for specific clients. Of course, many smaller companies, particularly small eCommerce companies, do not have the budgets to invest in this way and so should tailor their budgets to the most appropriate FDP solution for them.

1.2.2 Implement Mobile Security As Soon As Possible

With mobile payments fraud increasing rapidly, it is imperative that merchants and FIs invest in securing their mobile channel sooner rather than later.

An additional problem for many companies is the security threat posed by BYOD (Bring Your Own Device), as employees connect and access corporate data using their own devices.

Although fraud via smartphones is increasing at a faster pace than general PC/laptop based fraud, smartphones have the potential to become as secure a channel as the web through the use of advanced encryption and authentication technologies. This typically involves leveraging key smartphone sensors such as accelerometers, cameras, GPS receiver, microphone and fingerprint/iris sensors to provide advanced biometric security.

Following the publication of the new FIDO (Fast Identity Online) Alliance UAF and U2F standards, the biggest players in financial services, eCommerce and consumer electronics industries, such as MasterCard, Visa, Google, Samsung and Microsoft, have already started to use biometric authentication as a replacement fort passwords, thus following in the footsteps of Apple which has featured biometric identification in its smartphone products since 2013.

1.2.3 Merchants & FIs Must Provide A 'Frictionless' Secure Payment Experience

It is imperative that eCommerce companies and FIs achieve the right balance between the use of FDP tools to catch fraudsters on the one

hand and converting legitimate website visits into sales on the other. It is critical to ensure that innovations are in fact creating what consumers really want; frictionless, secure, payment experiences.

However, this is not always an easy balance to achieve, despite the sophistication of current FDP solutions.

1.2.4 Develop Fraud Prevention Investment Strategy

Investment in FDP solutions varies widely, ranging from a few thousand dollars per annum for small merchants (with a relatively small number of transactions per day), to hundreds of thousands, or even millions, of dollars in the case of some of the biggest online banks (based on the numbers of active online banking users).

However, FIs and merchants should understand that the licensing of software is usually only one part of a much larger FDP investment strategy that includes educating employees and customers, marketing, system configuration, call centre support, etc.

1.2.5 Cross-industry Collaboration is Required to Effectively Reduce Online Fraud

Merchants, issuers, acquirers, processors and service providers have for years recognised the need to take a collaborative approach when tackling online fraud. However, existing legislation seems to foster a 'pass-the-parcel' approach (where one party legitimately passes fraud liability to another) rather than a collaborative approach.

There is a wealth of information available across the electronic payments ecosystem and that information could collectively be used to combat fraud.

If the payments industry is to seriously disrupt fraudsters, then it is vital that all the relevant parties take a wider, shared approach to the problem and commit to combating fraud at the enterprise and the industry level.

2. eCommerce Fraud: Market Overview

2.1 What is Driving Fraud in eCommerce & Online Banking?

Fraud affects the entire electronic payments value chain, spreading rapidly across geographies and industries. It also increases costs, reduces revenue, damages reputations and degrades customer experience.

Although it is a problem for both CP (Card Present) and CNP (Card Not Present) transactions, card fraud is bigger problem for online payments, ie eCommerce CNP transactions. In Europe, around 60% of card fraud is associated with CNP transactions.[i] The main drivers behind fraud in eCommerce and online banking are:

- Growth in eCommerce – eCommerce has become mainstream and is forecast to expand rapidly during the next few years. Factors driving this growth include advanced shopping, payment options and brands pushing into new international markets.
- Increasing flows of money – whether through traditional online, mobile or cross-channel inevitably captures more attention from fraudsters.
- Increased use of mobile payments – the increasing use of smartphones for payments is a significant factor driving the volume of eCommerce sales, particularly in emerging markets.

  In developing countries with immature payment services and limited fixed line Internet penetration, people are increasingly using mobile phones to access the Internet, shop and move money. In some of these markets, mobile may be a primary channel for these activities.

- Increased number of serious data breaches – fraud trends are largely driven by the vast quantities of identity data available to cybercriminals after data breaches. 2015 was a record year for data breaches with well-known consumer brands such as TalkTalk in the UK and T- Mobile in the US being subjected to attacks.

  Successive data breaches across many organisations mean fraudsters can now build very complete identity information on their victims. The data is rich enough for them to apply for and successfully open a bank account in the victim's name. This is why there is such a surge in account application fraud.

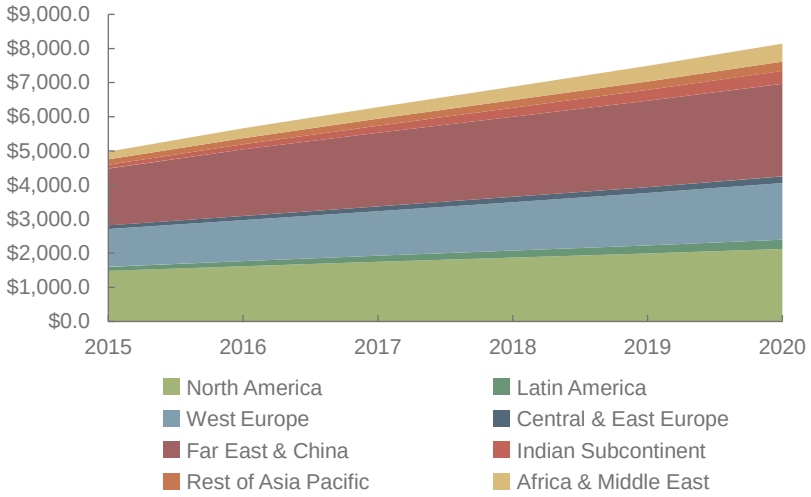
  Fraudsters are increasingly concentrating their efforts on obtaining personal and financial details from individual customers rather than obtaining this data by directly attacking the banks.

- Technology introduction – with the US finally having adopted EMV to protect CP POS purchases, it is likely that fraudsters will switch their attention to CNP purchases.

2.1.1 Growth in Global eCommerce Fuelling Fraud

Global eCommerce sales continue to increase rapidly across the world and inevitably this will result in an increase in fraud, despite the best efforts of eCommerce merchants and FIs. In terms of transaction value, the total eCommerce market was valued at under $ 5 billion at the end of 2015 and is forecast to reach $8.1 billion by the end of 2020 with North America and Far East & China regions dominating the market throughout the forecast period.

Figure 2.1: Growth in eCommerce Transaction Value ($ billions) by Region



Source: Juniper Research

In terms of sectors, the eCommerce market is dominated by the banking and both physical and digital goods sales, which together amounted to 83.5% of the total market in 2015. Despite the growth of other sectors such as coupons, ticketing and gambling, during the forecast period, it is forecast that banking and goods sales will be 76% of the eCommerce market by 2020.

2.2 Global Fraud Rates

According to data from ACI Worldwide,[ii] the number of fraud attempts based on total population in 2015 increased to 1.49% compared to 1.39% in 2014, ie 1 out of every 67 transactions was a fraudulent attempt in 2015 compared to 1 out of every 72 transactions in 2014. This was a 7.1% increase during the year.

ACI also analysed fraud data during the 2014 and 2015 holiday shopping seasons starting on 27th November (Black Friday) and ending on 31st December. In both years, fraud attempts soared on key dates. The data is based on hundreds of millions of transactions from global retailers.

- During the 2015 holiday shopping period, fraud attempts were highest on Christmas Eve (2.4%), Thanksgiving (2%), Black Friday (1.8%) and holiday shipment cut-off days (1.6%). This is thought to be due to 2 key trends:

  a) Electronic gift cards, which had the highest fraud attempt rates across all products, were a popular last-minute gift purchase

  b) Buy online/pick-up in-store, which has a higher fraud attempt rate than other modes of delivery, increased 47% compared to 2014. Next day and overnight delivery fraud also increased by 50%.

According to the US National Retail Federation, the average online spending per person during 2015 holiday shopping season was $805.

Mobile devices are becoming increasingly popular for online purchases. However, fraudsters know that the mobile channel is more vulnerable than PCs/laptops, as many organisations have yet to apply the same levels of protection as they have in the web channel.

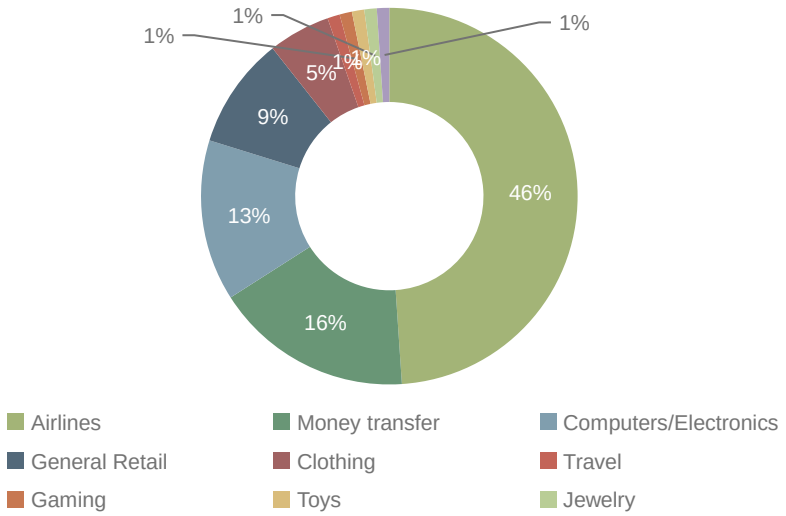
In 2015, approximately 42% of all consumer eCommerce transactions were initiated from a mobile device in the US according to the RSA Anti-Fraud Command Center.[iii] In the same year, the number of fraudulent

transactions on mobile devices increased by 142% compared to 2014; however, web-based fraud increased just 3% during the same period.

2.3 Fraud Attacks by Vertical & Region

According to data from RSA,[iv] the merchant categories most affected by eCommerce fraud, with 46% of fraudulent transactions, were airlines and travel, followed by money transfer at 16% and computers/electronics at 13%.

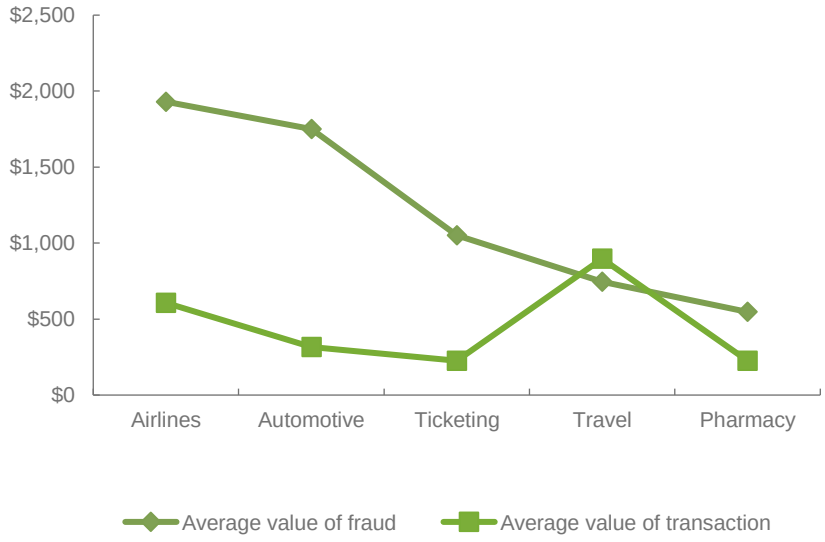
Figure 2.2: Top Merchants Affected by Fraud Transactions



Source:RSA Security

It was also found that the average value of a fraudulent transaction is significantly higher than that of an average legitimate transaction. For example, in the case of airline tickets, the average legitimate ticket purchase is $606, whilst the average fraudulent ticket purchase is more than 3 times higher at $1,930.

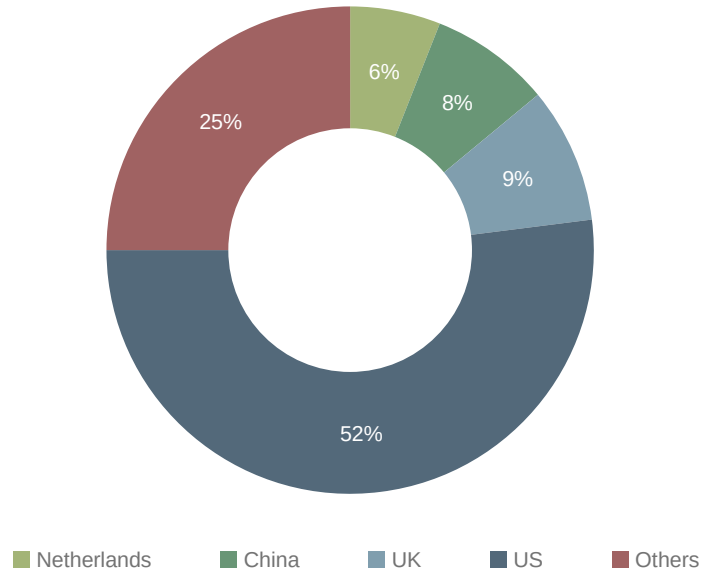
Figure 2.3: Average Value of Fraud Transactions



Source:RSA Security

In terms of attack volume, the top countries targeted by fraudsters in September 2014 were the US, the UK, China and the Netherlands This was 75% of total attack volume (see figure 1.7 below).

Figure 2.4: Top Countries by Attack Volume



Source:RSA Security

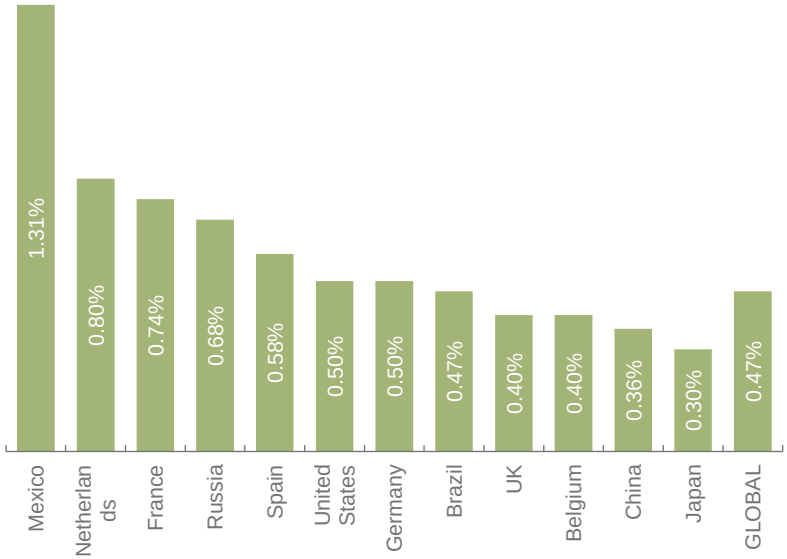
Meanwhile a study carried out by Ingenico found that the countries with the highest online fraud rates (as measured by fraud chargeback rate) were Mexico, the Netherlands, France and Russia (see figure 1.8).

In Mexico, the high fraud rate is due to an exceptionally high fraud 'climate,' merchants' lower eCommerce maturity and the failure to use 3D Secure which results in fewer opportunities for merchants to shift liability.

In France and the Netherlands, online merchants have only recently started to develop expertise and fraud prevention tools to tackle online fraud more effectively.

In the US and UK, online merchants have had a longer experience of dealing with fraud issues and therefore address the online fraud problem with more focus than other countries. The chargeback rates for these 2 countries are near to the global rate of 0.47%.

Figure 2.5: Percentage of Transaction Value Reported as Fraud Chargeback by Country (Large Corporate Companies)



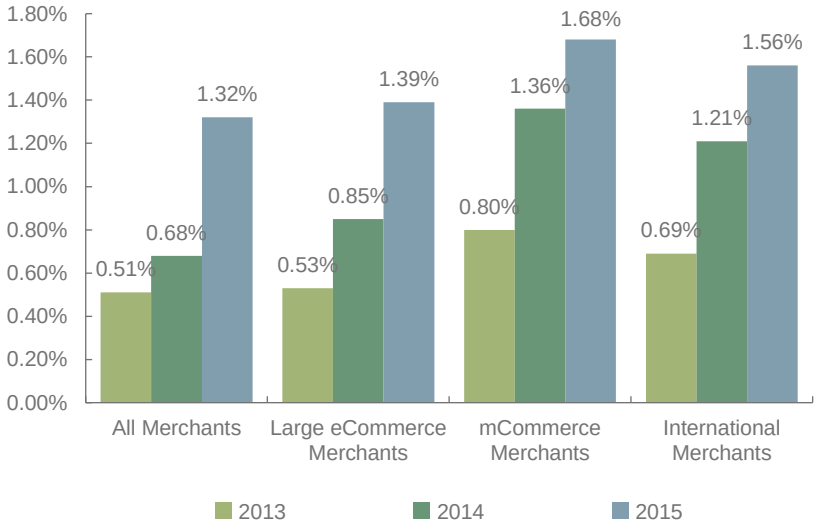
Source:Ingenico Payment Services

2.4 The Cost of Fraud

Online commerce (ie CNP transactions) is more vulnerable to fraud than traditional CP commerce at a POS and can be very costly for merchants. Estimated costs, depending on vertical and region, vary between 0.3% and 3% of revenues.

According to a 2015 survey by LexisNexis, merchants claim that fraud losses are increasing despite the companies investing more in fraud prevention.[v]

Figure 2.6: Fraud loss as a Percentage of Revenues in North America, 2013-2015



Source:LexisNexis

In 2015, large eCommerce merchants lost 1.39% of revenue to fraud on average, despite spending, around $115,000 annually on fraud mitigation. However, it is the mCommerce and international merchants that reported the highest fraud losses at 1.68% and 1.58% respectively.

The costs shown relate to the replacement cost of goods due to fraud, which will vary according to the type of goods, with physical goods clearly being a much higher cost than digital goods.

As can be seen from figure 1.9, there was a substantial increase in revenues lost for merchants between 2014 and 2015, averaging 94% across all merchants.

However, the true cost of fraud will include other costs such as:

- Shipping and insurance costs.
- Investment and operational costs of deploying an FDP solution.
- Manual review costs – costs of internal staff to review suspicious transaction. This will vary from company to company and will depend on the manual review rate set by the company.
- Chargebacks – a chargeback is a demand by a credit card company for a retailer to make good the loss on a fraudulent or disputed transaction. Chargebacks can occur up to 6 months after the transaction and must be reimbursed by the merchant that processed the order.

  In 2014, the average global fraud chargeback was 0.47%, ie the percentage of total transaction value reported as fraud chargeback.

When the above factors are included, LexisNexis estimates that in 2015 the true or total cost of fraud for online merchants was $223 for every $100 of goods lost.

2.4.1 Manual Checking

If a transaction is flagged as high-risk, it may be submitted for a manual check by a review team. The team will have additional data verification sources and may apply their own judgment, developed through experience, to make a decision.

Despite the use of sophisticated FDP solutions, fraud mitigation is still very much a manual process. Even among the 25% of merchants using FDP systems to flag fraud, three-quarters of flagged transactions are ultimately resolved by internal staff.

The average manual review rate across all merchants is around 27%, with around 2.3% of orders rejected.[vi] The manual review rate varies according to the size of the merchant, with the largest merchants applying a manual review around 7% of orders whilst the smallest merchants review around 42% of all orders.

Table 2.7: Variation in Manual Review & Orders Rejected Rates with Merchant Size

Merchant Revenue	Less than $5	$5 to $25 million	$25 to $100 million	Over $100+ million
Manual Review Rate	42%	25%	24%	7%
Orders Rejected (%)	1.6%	4.5%	1.9%	2.5%

Source:Visa Europe

Merchants selling physical goods reject slightly more suspicious orders than other types of merchants. This is because a fraudulent order typically costs them more, owing to the higher cost of the goods sold plus the shipping costs, to which other merchants are not exposed.

In combating fraud, merchants must think about the customer and ensure his/her experience is not compromised. Blocking suspicious purchases without detailed evidence or introducing complex, user-unfriendly measures can lead to ‘cart’ or ‘basket’ abandonment.

In particular, this involves trying to minimising the number of false positives, the legitimate transactions that are declined. In many cases, the rate of false positives flagged as possible fraudulent transactions can be 25% of all flagged transactions, which can be higher for international merchants.

Ultimately, this is a balance between introducing intentional friction to gather enough evidence to trust a consumer’s identity and providing a hassle-free buying experience for the customer.

2.5 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 a 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 in combating 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.
- 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 licences. 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 phony 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 practise 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 organisation, 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.

2.6 Use Cases

FDP solution vendors provide software solutions that address many different types of use cases, some of which are very specific to their customers' individual businesses. However, in general the most common use cases are:

- New account fraud
- Account takeover fraud
- Payments fraud (across all payment types, networks and all channels)
- Loyalty and promotion abuse
- Internal fraud abuse (staff and collusion)
- Supply chain abuse (returns and claims)

3. Overcoming the Fraud Challenge

3.1 Introduction

Fraud is a global problem and fraudsters are becoming increasingly sophisticated. Whereas in-house FDP solutions might have been adequate to keep fraud to a minimum level a few years ago, this is no longer the case today. Fraudsters need to be with dealt by means of sophisticated, real-time fraud screening solutions, supported by an understanding of the latest fraud patterns and behaviours around the world.

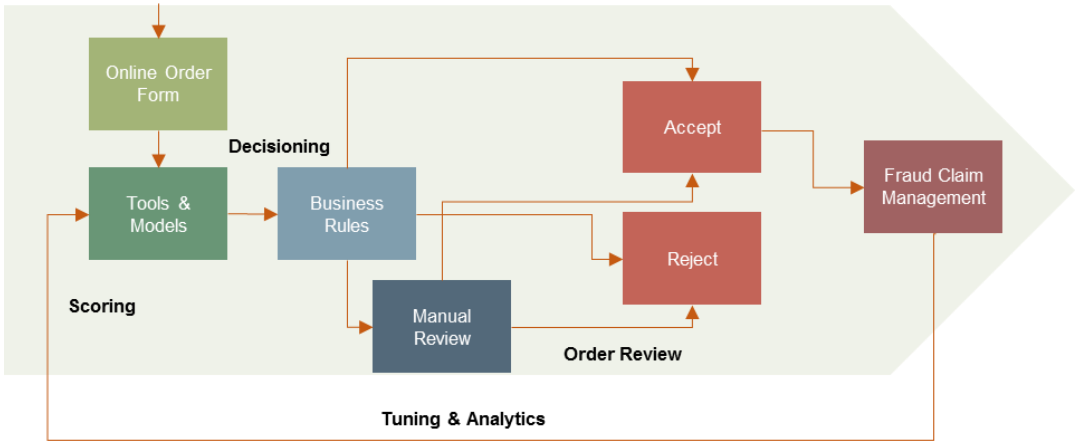
The most common fraud attack use cases are new account origination, account takeover and payment fraud. With account takeover and new account fraud detection, organisations attempt to discover unauthorised or fraudulent users posing as legitimate users, whilst payment fraud detection involves determining whether purchases are being, or have been, made with stolen payment cards.

In addition, most vendors increasingly offer fraud intelligence services, authentication, malware detection (such as MitB [Man-in-the- Browser] infections on mobile devices), as well as managed services in which the vendor is primarily responsible for monitoring and taking action in instances of fraud.

3.2 How Does a FDP System Work?

FDP systems run background processes that scan transactions, score them based on the possibility of fraud and then make a decision on whether to accept, decline or submit the transaction for further analysis. Essentially, they must be able to detect when a person logging in is who they claim to be and detect anomalies from normal authentication behaviour.

Figure 3.1: Schematic Overview of FDP Solution



Source: Juniper Research

The basic elements of a FDP solution are:

- Order Reception– an order is received by an eCommerce company and the associated transaction information such as customer name, address, CVS and AVS codes, etc, which form the 'raw' data or original data fields are collated.
- Tools & Models – a number of fraud detection and authentication tools are employed.

The resulting data is fed into a risk model and a risk score is generated. Vendors typically offer their customers a number of different risk models based, for example, on region and type of vertical.

Many different datapoints are considered to determine the score, such as device ID, other device characteristics, geolocation, user behaviour, order links and so on. The data is then compared against 'normal' attributes.

After the use of many fraud detection and authentication tools, the number of data fields may increase to more than 300 compared to 20 at the order reception stage.

- Data Analysis & Resolution – this is where a decision is made on whether to accept, decline or submit the transaction for further analysis or review. Resolution may employ a rules-based model, a behaviour-based model or increasingly a combination of the 2.

  Example of a rule:

  a) Automatically block customers who try to pay over a VPN. VPNs can make an IP address look like it is coming from another location, a common practice among fraudsters overseas who want to make orders look as if they are coming from within a country.

  b) If the transaction is deemed valid, it is allowed and processed. If the transaction falls outside an accepted range, an alert is issued and the transaction may be sent for manual review or automatically suspended or denied.

- Manual/Automated Review – a transaction may be suspended and sent for manual review if the actual behaviour is out-of-range with what is expected. This can range from asking users to re-authenticate themselves, either by calling them directly or by connecting with them automatically.

  Automated follow-up is often done by using another channel, such as sending an OTP to a user's mobile phone, or more commonly by asking a user to answer one or more 'secret' questions that only the legitimate user can answer correctly. Some FDP vendors offer these additional authentication and transaction verification capabilities, whilst others do not.

- Fraud Claim Management – typically business rules are adjusted manually, either by the bank/merchant or by the FDP vendor, to take account of new developments. A small number of advanced FDP solutions have developed the capability to take out the guesswork of establishing new rules and optimise the configuration of rules. These systems can also test new business rules configuration against historical data.

3.3 Key Challenges

3.3.1 Organised Criminal Networks

Fraudsters are more sophisticated than ever. Fraud has evolved from individual rogues to organised criminal networks operating in countries across the world.

In fact, merchants and FIs often end up several steps behind fraudsters due to the fact that they are more constrained by regulation, budget, personnel and red tape amongst other. These constraints pose considerable difficulties for these organisations compared to the fraudsters, who are not limited by such constrains.

Fraud is increasing as a percentage of total revenues, despite the fact that organisations are investing more in FDP solutions. A particular problem is cross-channel fraud. Fraudsters know that most bank fraud systems rarely monitor customer behaviour across multiple accounts, channels and systems. This vulnerability paves the way for cross-channel fraud, in which criminals gain access to customer information in one channel and then use it to commit fraud in another channel. However, an increasing number of FDP vendors are offering solutions that monitor cross-channel fraud.

3.3.2 Awareness

FDP solutions vendors claim that many organisations in the eCommerce industry, particularly small and medium sized businesses relying on inferior in-house solutions, are unaware of the availability and capabilities of FDP solutions, so FDP vendors need to urgently increase awareness of their solutions.

3.3.3 Investment in FDP Solutions

Fraud increased for eCommerce merchants in 2015, with all merchant segments losing more revenue compared to 2014, despite increased spending on FDP solutions, which many merchants believe are expensive.

In response, vendors are increasingly offering their technologies on a SaaS basis, reducing the initial capital expenditure needed to deploy FDP solutions, so making it easier for some of the smallest merchants and banks to protect themselves.

Investment in FDP solutions varies widely, ranging from a few thousand dollars per annum for small merchants (with a relatively small number of transactions per day), to hundreds of thousands, or even millions, of dollars in the case of some of the biggest online banks (based on the numbers of active online banking users).

However, the licencing of software is usually only one part of a much larger fraud prevention investment. Merchants and FIs that do not understand the total commitment required are reticent to invest further, whilst companies that do understand the size of the commitment necessary to get substantial benefit are often overwhelmed by the sheer scale of the effort.

3.3.4 Privacy Concerns

Another issue in fraud prevention is the potential ‘Do-Not-Track’ legislation introduced by the US Federal Trade Commission (and similar legislation elsewhere) designed to protect consumer privacy. The main objective of the legislation is to empower consumers to block attempts by online companies to collect personal data, particularly with respect to behavioural advertising.

The fraud prevention industry believes that companies engaged in cybersecurity should not be included in this legislation. Although some users are concerned about their information being used for advertising purposes, the fraud industry argues that consumers may be less concerned if their information is being used for transaction security purposes.

In fact, the importance of cybersecurity and the nature of the data collected requires that it be treated differently to consumer data collected for advertising purposes. Any Do-Not-Track legislation could bring with it some unintended economic and security consequences. For example, if companies are required to disclose the manner in which the collected information is used, it could expose the techniques used to discover risk of fraudulent activity to fraudsters, enabling them to develop workarounds or alternative technologies.

3.3.5 Cross-industry Collaboration Required

Merchants, issuers, acquirers, processors and service providers have for years recognised the need to take a collaborative approach when tackling fraud. However, existing legislation seems to foster a ‘pass-the-parcel’ approach (where one party legitimately passes fraud liability to another) rather than a collaborative approach.

There is a wealth of information available across the electronic payments ecosystem and that information could collectively be used to combat fraud. If the payments industry is to seriously disrupt fraudsters, then it is vital that all the relevant parties take a wider, shared approach to the problem and commit to combating fraud at the enterprise and the industry level.

4. Online Payment Fraud: Vendor Assessment

4.1.1 Vendor Assessment

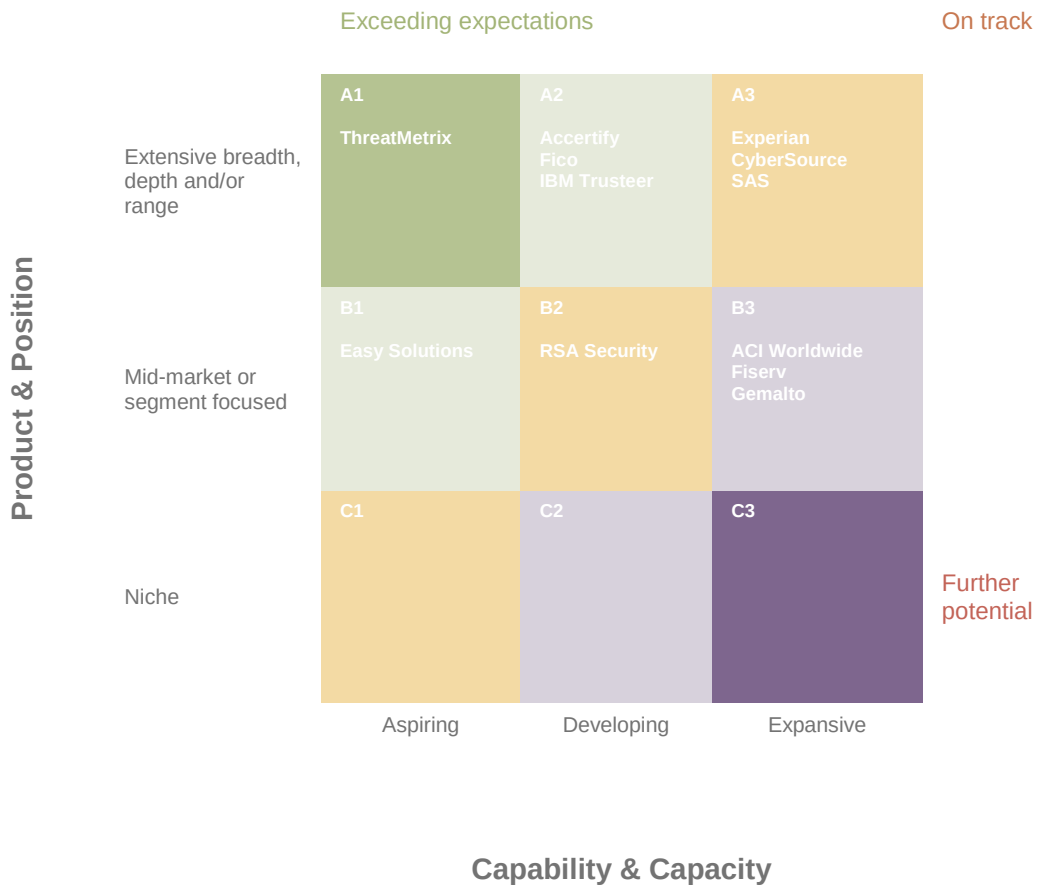
The approach with vendor assessment is to use a standard template to summarise vendor capability. The template concludes with our views of the key strengths and strategic development opportunities for each vendor. We also provide our view of vendor positioning using our Vendor Matrix technique. This technique, which applies quantitative scoring to qualitative information, enables us to assess each vendor's capability and capacity and its product and position in FDP. The resulting matrix exhibits our view of relative vendor positioning. We have assessed each vendor's capabilities against the following criteria:

Table 4.1: Vendor Capability Assessment Criteria

Category	Criteria	Description
Corporate Capability	Corporate Financial Performance & Size	In assessing this factor we have considered the absolute size of the vendor as measured by revenues, employees and investments.
	Financial Performance & Size in eCommerce	The size of the vendor in the eCommerce industry, in general, based on revenues, partnerships or customers announced.
	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 & Partnerships	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.
Strategic Position in Mobile & Online Banking	FDP Product Range & Experience	This factor relates to breadth of product range coverage by platform, technology and channels. We also evaluate the vendor's success to date, as measured by their experience and expertise with Mobile Network Operators, banks and FIs.
	Number of Online Banking & Merchant Customers	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.
	Experience: Clients & Strength of Partnerships	We consider here the extent to which the vendor has developed channel, product and wider industry relationships that will help increase market penetration.
	Creativity & Innovation	This factor assesses the vendor's perceived innovation through its flow of new features, products, developments and enhancements.

Source: Juniper Research

Figure 4.2: FDP Vendor Positioning Matrix



Source: Juniper Research

Table 4.3: FDP Vendor Matrix Scoring Chart

	Corporate Capability				Product Positioning			
	Corporate Financial Performance & Size	Financial Performance & Size in Sector	Operations & Global Reach	Marketing & Partnerships	FDP Product Range & Experience	Customers	Clients & Strength of Partnerships	Creativity & innovation
ACI Worldwide								
Experian								
ThreatMetrix								
CyberSource								
Easy Solutions								
Accertify								
RSA Security								
FICO								
IBM Trusteer								
Fiserv								
Gemalto								
SAS								

Source: Juniper Research

4.1.2 Experian

Juniper interviewed Teresa Grove, Global VP Product Marketing, Experian Decision Analytics and David Britton, VP Industry Solutions at 41st Parameter in February 2016.

i. Corporate

Experian is a global information services company which provides data and analytical tools to client companies around the world. Based in Dublin, Ireland, it is a publically listed company and trades on the London Stock Exchange. It had revenues of $4.8 billion in 2014.

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.

Fraud detection and prevention activities are contained in the Decision Analytics division. 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.

In April 2013, Experian acquired Decisioning Solutions, which became the core of its Decision Analytics platform. This unit provides credit and non-credit data, customer analytics and fraud detection to lenders, cable and satellite companies, telecoms firms, third-party debt collectors, utilities and state and federal government entities.

In October 2013, Experian acquired 41st Parameter, 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. High-level View of Products

Experian offers its own authentication products developed in-house, as well as products developed by 41st Parameter.

Experian's main fraud platform is known as FraudNet, which is based on technology developed by 41st Parameter. Customised 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 analyses 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 represented in establishing a new account.
- FraudNet for Account Takeover – a fraud management application that provides for account takeover activities.
- FraudNet for Transactions - a rules-based risk engine that analyses transactions to determine the level of risk.

- Device Insight for Payments – a solution which can identify every device which tries to connect to an online payments platform on every visit.
- FraudNet and PreciseID - a cross-channel platform which provides companies with the ability to manage fraud risk associated with traditional identity information (PreciseID) coupled with device-based information (FraudNet) through a single platform regardless of channel.

According to Experian, the main benefits of the combined products are significantly reduced false positives, improved operational efficiencies and a much improved customer experience.

iii. Business Model

The FraudNet platform is offered in a SaaS-based hosted environment. Unlike some of its competitors, every Experian customer operates in a hosted environment. This not only applies to eCommerce customers, but also all banks and financial services customers. In fact, Experian claims that it was the banks that insisted that Experian offered a hosted platform as they did not want to bear the IT burden themselves.

However, there is an element around the device recognition technology, the device collector technology, which resides on-premises with customers.

iv. Key Clients & Strategic Partnerships

- Experian has a wide range of partners, the majority of which are not publically disclosed. Key publically announced partnerships include with ACI WorldWide, FICO and Symantec. For instance, mobile payments company ACI 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 organisations.

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

- 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) minus all the false positives.
- 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 analyse the characteristics and configuration of devices used to make payments. The company believes that a rules-based risk engine is more accurate than a behavioural-based engine in a real-time fraud detection environment. However, the company does use behavioural analytics and Big Data offline.

- Another of its key strengths and differentiators is its cross-channel capabilities as its solutions includes online, mobile web, mobile app, call centre, in-branch and kiosk capabilities

Endnotes

[i] European Central Bank, 4th Report on Card Fraud, July 2015

[ii] http://www.securitymagazine.com/articles/86878-holiday-season-e-commerce-fraud-rates-rise

[iii] https://community.rsa.com/docs/DOC-40326

[iv] Bring on CyberMonday: E-Commerce Merchants and Fraud, October 2014; https://www.emc.com/collateral/fraud-report/resa-online-fraud-report-102014.pdf

[v] 2015 LexisNexis Risk Solutions True Cost of Fraud Study, September 2015

[vi] CyberSource Online Fraud Management Benchmarks, North America