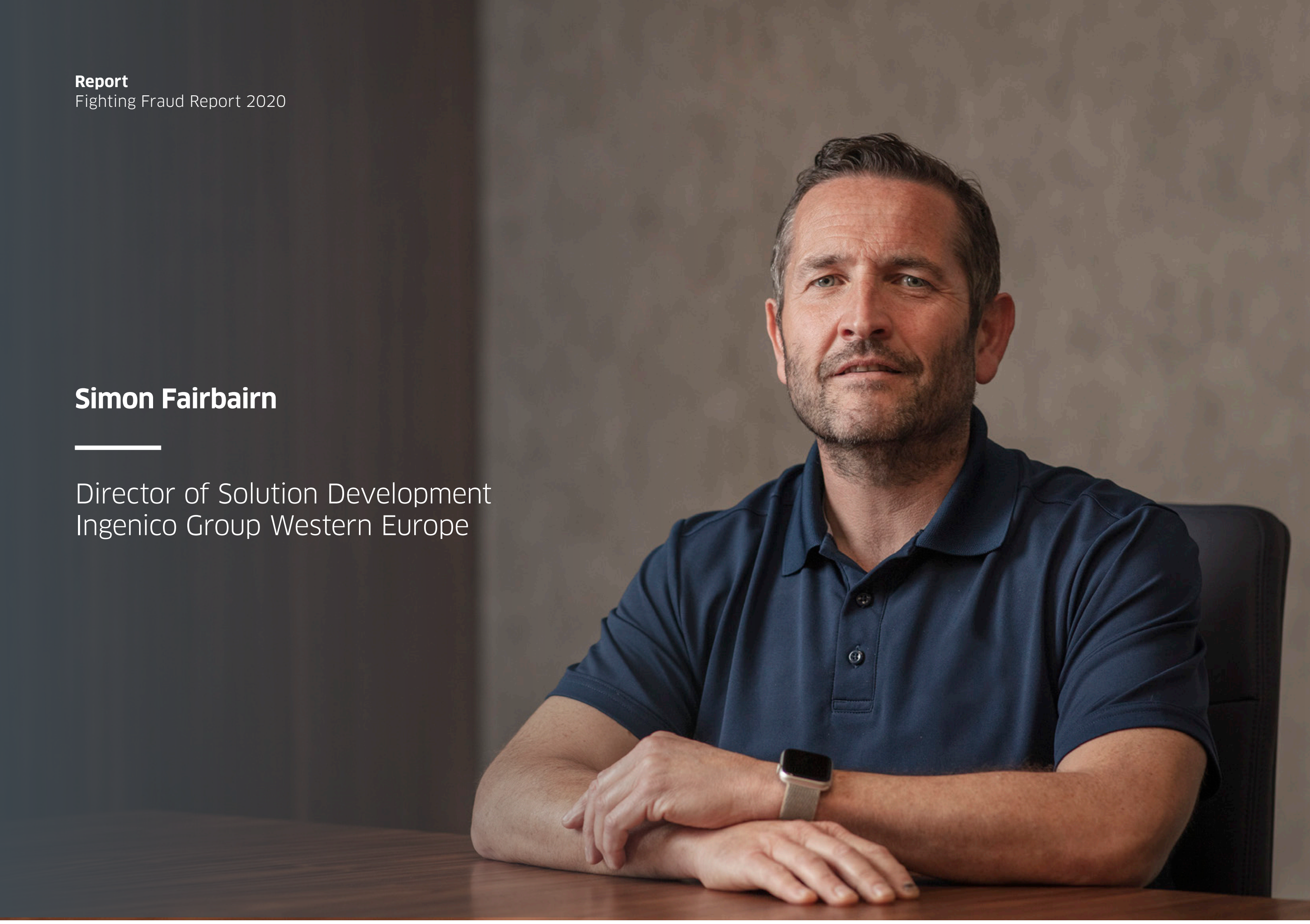
Fighting Fraud Report 2020

Tackling the changing threat of instore payment fraud



Simon Fairbairn

Director of Solution Development
Ingenico Group Western Europe

Foreword

We all know that fraud is a threat that never sleeps.

The payments industry, and the merchant and consumer ecosystem it supports, is locked in a relentless battle against the criminals that want to harm businesses and consumers for their own gain.

To defend against instore fraud, the entire ecosystem – retailers, acquirers, schemes, technology providers and payment experts – must work collaboratively. In creating the Fighting Fraud Report, we at Ingenico want to foster a spirit of collaboration. We want to start a conversation about fraud, bringing people from across the industry together to share insight and approaches.

It would be impossible to give a totally comprehensive history of instore fraud. However, in this report we have compiled a detailed summary of fraud up to the present, the various solutions that have been developed to tackle it, an explanation of the innovative new technologies being utilised against fraudsters, and how fraud is expected to evolve in the future.

This information will be invaluable to anyone working in the banking and acquiring space today, as well as retailers with physical outlets under threat from criminals. Understanding the evolution of fraud will help you anticipate where the next risks will come from. Reading first-hand accounts of how businesses are utilising innovative technology to combat fraudsters will suggest approaches and solutions that you could implement in your own organisation and with merchant partners.

The 2020 Fighting Fraud Report is intended to act as a baseline, the first in a series of papers and reports in which we will explore instore payments fraud and the evolving omnichannel context that now surrounds it. We will introduce commentary and insight from industry leaders and experts that we can all benefit from.

We're looking forward to discussing this topic with our customers and partners throughout the year, and sharing more content in the coming months.

Contents

£1.2 billion

Amount stolen through fraud in the UK in 2018
Source: Fraud the Facts 2019

£4.13

The cost to retailers of every £1 of fraud
Source: LexisNexis

1: Introduction

Payments fraud is a growing issue for merchants, issuers and acquirers. Fraud losses can have an enormous impact on the bottom line for businesses across the payments ecosystem. However, beyond any immediate financial loss, consumer trust and business reputation are also at risk. Fraud is often devastating for the customers – people who, let's not forget, have had their money and sometimes their identities taken from them. The long-term damage to the brand caused by fraud can be enduring and toxic. The stakes are high in the fight against fraudsters.

Nowhere has the digital revolution been more apparent than in the relationship between customers and merchants. Whereas other industries have seen greater efficiencies, often radical transformations, the consumer-merchant relationship has expanded, deepened and dramatically reconfigured. Consumers want to transact wherever, whenever and however they chose, and the industry is utilising the latest technology at its disposal to offer an increasingly innovative array of channels, payment methods, loyalty incentives and fulfilment options.

Alongside this increase in consumer choice, the EU Second Payment Services Directive (PSD2) has levelled the playing field by creating new categories of payment services and lowering barriers to entry. A rapid revolution in consumer payments is occurring; the majority of European markets (and even more so in Asia) have seen a reduced volume of cash payments, with cards and alternative payments proving increasingly popular. In the UK, the value of retail purchases made by card last year accounted for more than three quarters of all retail sales[1] and one in three transactions (roughly 20 million per day) are now contactless.[2] Much of this change is powered by the speed, convenience and security that cards can offer consumers with increasingly busy lifestyles.

What is fast fraud?

Many of the goods and services we buy now are no longer just physical, they're digital. But customer expectations of digital goods are different; while we might be happy to wait 24 hours for delivery of a shirt bought online (and even that's not quick enough for some these days), we expect digital goods to be delivered instantly.

But this is something that fraudsters can exploit. Most traditional payment solutions don't have the speed necessary to carry out fraud prevention measures and deliver digital goods instantly. Criminals exploit this to quickly steal digital goods that can be sold through secondary markets.

While the industry has taken significant strides to combat card fraud, criminals continue to successfully adapt their approach

But, as consumer payments evolve, so too does fraud. Payment cards, regardless of type, have offered fraudsters a lucrative avenue over the years, with the opportunity to clone, counterfeit and generally misuse stolen card details to make money. While the industry has taken significant strides to combat card fraud, criminals continue to successfully adapt their approach to find new and ever-more resourceful ways to exploit any gaps in payments security. Today's fraudsters are more intelligent and organised than ever, often comprised of strings or even hierarchies of fraudsters involved in large, complex fraud attacks.

In 2018, criminals successfully stole £1.2 billion through fraud in the UK alone.[3] The impact of these losses isn't limited to the value of goods or services obtained by fraudsters either. Research has shown that, in 2018, every dollar of fraud cost retailers $2.94, which is a 6% increase from 2017. Additionally, the level of fraud as a percentage of revenue has increased, particularly for financial services firms, who are starting to feel the effects of "fast fraud" and its associated costs.[4]

The indirect costs that hit merchants, issuers and acquirers as a result of fraud include the resources required to manage the chargeback, investigation and reporting procedures, as well as additional processing costs. High levels of fraud can also potentially result in scheme fines, an impact on insurance, reputational damage and even loss of merchant accounts. For these reasons, it is imperative that merchants and financial services providers keep payments security at the top of their agenda and continually work to understand changing fraud trends.

Our intention with the Fighting Fraud Report is to provide ongoing information about the most advanced solutions and techniques for fighting fraud. In doing so, we plan to keep fraud at the top of the agenda and champion the fraud-prevention cause across the entire payments ecosystem.

The individual impact of fraud

We often discuss the impact of fraud in abstract terms, but what does it mean for the businesses involved? Over half (53%) of businesses in the EMEA region say they have experienced an increase in fraud over the last 12 months, which means financial losses for the businesses involved, not to mention the time and resource that must be dedicated to resolving fraud disputes.

However, instead of viewing fraud losses in purely financial terms, over a third (34%) of organisations consider the loss of customers to have a greater business impact. Customers are becoming increasingly aware of the vulnerability of their information - 46% of European consumers are concerned about the security of their financial data.

Expert Opinion

We need a more collaborative approach to fraud prevention

Fraud affects everyone, from consumers to businesses, and the costs and impacts are high. There is no doubt that criminals will continue to evolve their techniques to take advantage of the changing landscape within payments. They will target areas that are perceived to be weak, which could include technology, processes, third party suppliers, employees and consumers.

This is a challenging and complex space, but advancements in AI and transactional analysis have created great opportunities, alongside other tools, data sets and risk-based rules, to help experts identify genuine fraud over false alerts.

While the industry has done much to combat fraud, much more needs to be done across all areas of the payment value chain, including efforts from police, government and regulator and consumer groups, to ensure a focused and collaborative approach. Areas such as financial crime reporting and sharing of fraud data, as well as stakeholder training and awareness, could all be improved.

It's upon all of us in the industry to work together to protect our customers and businesses and ensure we are always ahead of the fraudsters.

Andrea Dunlop
Chair – EPA

Changes in consumer behaviour offer criminals more opportunities to hide their activities and exploit weaknesses

2: Tracking the path of payment fraud

Before exploring the latest trends in payments fraud, it is crucial to understand how the issue has evolved. By looking at the evolution of fraud, we can begin to forecast future fraud trends and take action to address them. Since fraud patterns adapt in line with consumer trends, reviewing the latter is the best starting-point.

The omnichannel evolution

Shoppers have embraced a growing number of channels and connected devices that offer them fast, convenient ways to find the items they want at the best price. Enhanced technology and connectivity over the last few years has seen consumers increasingly completing their buying journeys across a multitude of channels, often combining several of these channels to conduct a single transaction. With instore, eCommerce, mobile, telephone, mail order, social media and even IoT devices on offer as buying channels, consumers have an abundance of choice when it comes to making a purchase. As the barriers between these channels become more seamless, or even invisible, the omnichannel shopping journey will undoubtedly become the norm.

All these choices do not mean that the traditional bricks and mortar stores are irrelevant – in fact, research highlights that for omnichannel shoppers, 80% of purchases are still finalised instore.[5] For physical products, there is a comforting psychological aspect to being able to see something with one's own eyes before making a purchase. Not to mention the purchase often feels more secure to the buyer. There is also the reassurance of a personal interaction with another human being, especially if the customer requires assistance or has questions.

While the increase in channels is a customer-driven evolution, it is also welcomed by fraudsters. New channels and changes in consumer behaviour offer criminals more opportunities to hide their activities and exploit weaknesses. Fraudsters can stay below the radar by spreading many small frauds across multiple targets. Truthfully, do consumers meticulously audit all their transactions? With great choice comes a certain degree of fragmentation, and the perfect conditions for fraud to go unnoticed.

Expert Opinion

Fraudsters are being driven back instore

As SCA starts to make eCommerce fraud harder, fraudsters will direct their thieving back into the store. Whether it is 'Buy Online, Pickup Instore' fraud, use of stolen card numbers within a mobile wallet, some derivation of click-and-collect, or friendly fraudulent returns, the burden to merchants is only going to rise. A mix of the latest technology, tight and evolving processes, and training of informed, vigilant staff will help to prevent this burden becoming unacceptable.

Tony Craddock
Director General – Emerging Payments Association

A switch in fraud tactics

For many years, card-present fraud was a significant issue, with many credit, debit and prepaid cards being relatively simple to fake using stolen or false details. In the last decade, the introduction of enhanced security and legislation has begun to alter that pattern by making the fraudsters job harder and forcing them to look for alternative routes.

The growing uptake of EMV Chip and PIN has been instrumental in drastically reducing the volume of card fraud at the point of sale (POS), as well as at ATMs. EMV was mandated in many European countries over a decade ago (and latterly in the US in 2015), with the structure and function of the new cards and terminals, leading to an 80% reduction in card-present fraud.[6]

As this avenue began to close down for fraudsters, overseas merchants without EMV acceptance capabilities started becoming the targets for fraudsters looking to use counterfeit and stolen cards. However, fraudsters primarily switched their focus to card-not-present (CNP) transactions, where they could continue to use those details online, largely without significant security checks in place, except for where merchants were using 3D Secure or similar authentication methods.

Account takeover and identity theft have also been a popular focus for fraudsters for many years. By obtaining sensitive personal or financial data of a genuine shopper, criminals can intervene to take control of the consumer's account, or even use their credentials to set up a new account, in order to fraudulently obtain goods and services. This type of fraud can be particularly difficult to identify, since it uses genuine customer information – making it an attractive route for fraudsters and a particularly devastating one for merchants, financial institutions and their customers.

Account takeovers can be partially or entirely automated, meaning that they can be conducted on a huge scale. What's more, most account takeover attacks go unnoticed, and attackers take special precautions not to be detected. All of which means that it could be an ongoing drain on an organisation's bottom line without anyone even realising.

Expert Opinion

Fraud is a multi-faceted problem requiring a holistic approach

The three pillars of fighting fraud are people, process and technology. All three have equal importance. Most payment fraud attacks include an element of insider involvement and greater effort must be applied to reduce these threats. Business processes often offer security vulnerabilities and we regularly see entry through an unlocked, or weakly protected, back door (security patching, SQL injection and password management are practical examples). From a technological perspective, there is no 'silver bullet' available, but the fraud battle will only be won through greater investment in tech as human fraud prevention efforts can't scale sufficiently to meet the escalating volume and speed of attacks. I consider the key protection technologies to be AI, ML, biometrics, SCA, P2PE, tokenisation and PCI PTS v5 devices.

Merchants do understand the high financial and reputational costs, as well as the major impact on customers, but often still treat payment security as an IT compliance task, rather than as an ongoing organisational issue. Likewise, fraud prevention departments do not have the status or budgets they deserve. A key recommendation is for greater collaboration across the entire ecosystem, as fraud prevention should be a shared battle and not a competitive issue. In order to prevent card fraud, PANs must be removed entirely from all store, digital and back office systems. Card details should be tokenised and encrypted everywhere, never stored in the clear. This would prevent criminals monetising card details following a data breach. New instore payment options such as Pay@Aisle, Pay from Bank Account, QR codes and realtime payments offer great potential for merchants, but must be introduced carefully to avoid creating new opportunities for fraudsters.

It is unrealistic to expect criminals to give up. Therefore, the priority is to make sure your business has a holistic approach to fraud prevention, recognising that fraud always shifts to the weakest link.

Mark McMurtrie
Director - Payments Consultancy Ltd
Ambassador - Emerging Payments Association

Barriers to entry to fraud

Fraud takes many forms, with various levels of difficulty. As mentioned before, EMV Chip and PIN has drastically reduced card-present fraud. Nowadays, to fake an EMV card, a fraudster needs to be part of a sophisticated criminal network with specialist information, technology and the expertise to use it.

Other fraud methods are less complex. After breaching a business' network and stealing card details, hackers will put them up for sale on dedicated 'carding forums' on the Dark Web. Any person that knows how to access and transact on the Dark Web can buy some card details and follow a step-by-step guide on how to use the data to commit fraud.

Fraud networks can sometimes be as organised and complex as the businesses they seek to exploit. Other times, it could be an individual operating at home on a personal computer. Understanding the resources and manpower required for different types of fraud is crucial in figuring out how to fight it.

The Ingenico Perspective

Who are we fighting?

When we think about payment fraudsters, it's easy to picture lone wolves opportunistically pick-pocketing vulnerabilities. And when you start to learn about the Dark Web, it's easy to picture a chaotic environment - the online equivalent of a dodgy down-town market, filled with seedy shops selling forgeries, forbidden pharmaceuticals, stolen identities and coaching on the many paths to ill-gotten gains.

But when it comes to tackling fraud, which relies on a vast trove of stolen credit card numbers and personably identifiable information, it's important that our industry remains clear eyed to what it is – a market filled with businesses. There is supply and demand. There is feedback, complaints, rules, enforcement – all the things we'd expect in any industry.

It is important that we think about fraudsters and fraud rings as enterprises and acknowledge that they exhibit many of the same motivations, practices, strategies and aspirations as our own businesses. This perspective keeps us alert to the scale of the threat, and wise to what we are combating: structured systems of goods and services, knowledge and relationships.

And, as with any industry, the watch-words are 'profit' and 'efficiency'. Every time that the payments industry creates a sustainable barrier to a prevalent method of fraud, the cost of doing business goes up. Comprehensive, usable payment data and personally identifiable information sets get more expensive, and the knowledge of how to bypass those protections becomes a pricier commodity.

Adam Roberts
Head of Marketing Communications - Ingenico Banks & Acquirers, EMEA

52%

Amount of merchants using mobile who struggle to detect fraudulent attempts

75%

Of financial institutions say mobile fraud attempts have increased over the last year

Source: Payments Cards & Mobile

3: Emerging payment fraud threats

The omnichannel evolution and the growing popularity of digital services are driving the changes in fraud trends.

A world of data

While account takeover is still a popular activity for fraudsters, their methods of obtaining access to a genuine customer account are now broader, more varied and to some extent easier than before. Where a criminal may have previously obtained a physical bank or credit card statement, telephoned customer service or perhaps used a website to use those credentials to gain access, there are many more sophisticated and effective options available today. Phishing, malware, social engineering and scams can all enable fraudsters to gain access to card, eWallet or bank accounts in order to make purchases and obtain goods and services with ease.

Data is the most valuable currency in the digital world and for fraudsters it is now available in abundance. Each data breach can yield hundreds, thousands or even millions of customer records which are then quickly sold online to criminals looking to profit.

Malware, bots and other malicious data-mining programmes are also readily available to buy for those seeking to obtain personal information for fraudulent activities.

Omnichannel offers a place to hide

With card-present fraud, a criminal could walk into a store and walk away with a high-value item with less information than would be needed to order the same item online. However, with the proliferation of CCTV cameras and facial recognition technology, the physical presence of the fraudster in the act of committing a crime presents greater risk to the individual. If they get caught, it’s game over and there’s nowhere to hide.

What digital channels such as eCommerce sites and mobile apps offer is the opportunity to carry out fraud remotely, and with a considerable degree of anonymity for criminals. They do not need to present themselves in person and can disguise their identity with false details and alternative addresses without recourse. More information is required, but fraud can be carried out from anywhere in the world, in relative safety and obscurity.

Fraudsters are exploiting the increasingly complex buying journeys omnichannel retail offers

Mobile payments are a particularly high-risk area. A 2018 merchant survey revealed that 52% of merchants using the mobile channel were struggling with the ability to detect fraudulent order attempts, with many having no specific fraud prevention strategy in place to tackle the nuances of this growing channel. This is exactly the sort of opportunity fraudsters look to exploit, so it is no surprise that, in the same survey, more than 75% of financial institutions, as well as merchants, said that mobile fraud attempts increased last year.[7]

This is perhaps to be expected; mobile payments are a relatively new frontier and all emerging methods experience growing pains. Fraudsters can use emulation software so that transactions appear to come from mobile devices. Retailer apps may have security vulnerabilities that fraudsters can exploit – Starbucks notoriously suffered an attack in this way. And while mobile apps like Apple Pay and Samsung Pay come with fairly robust hardware and software protections (fingerprint scanning, tokenisation so no card details are saved on the device), it's still possible for malware to exploit bugs in operating systems to harvest the card information entered into the apps.

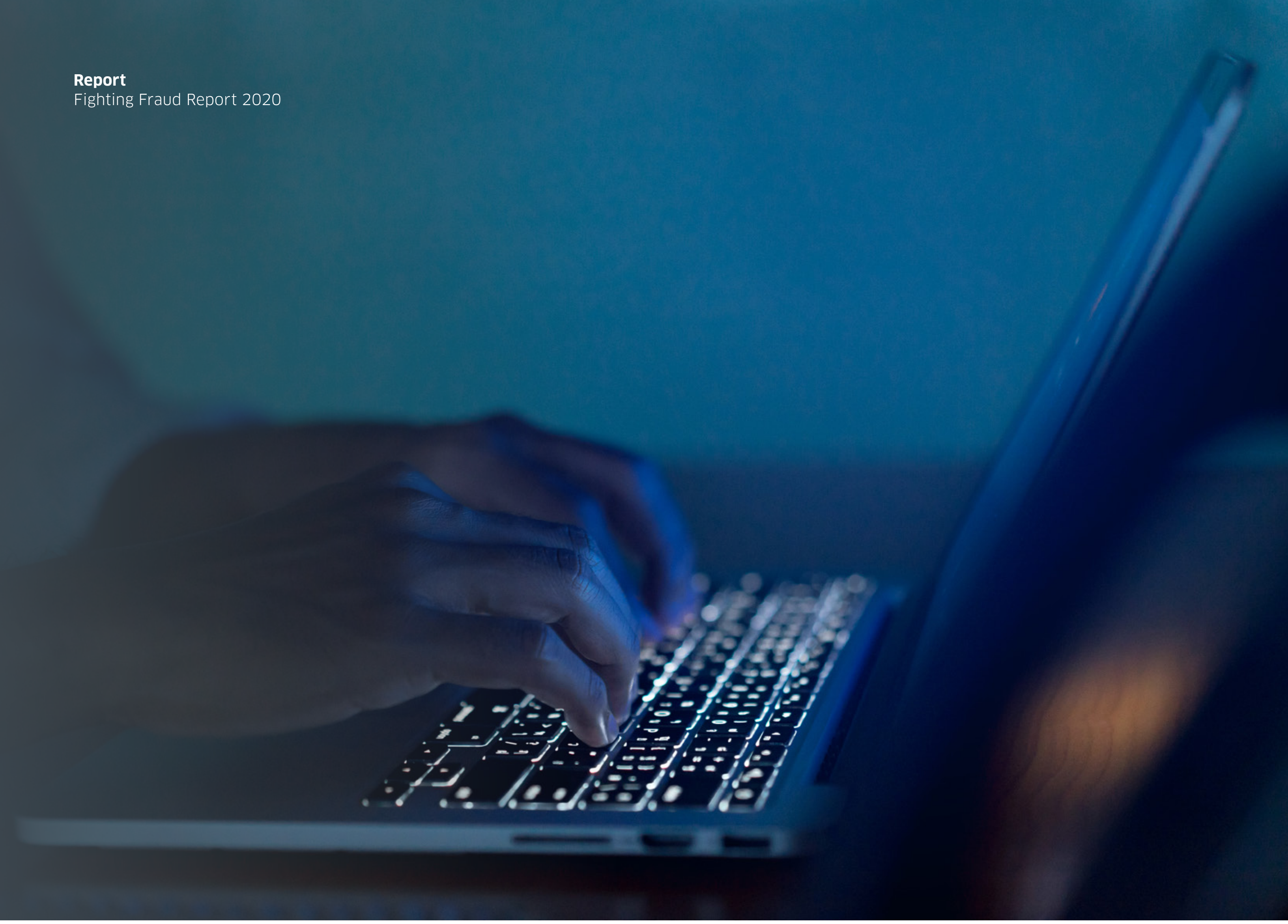
Online and offline are merging

What omnichannel increasingly means from a fraud perspective is that the lines between card present and card-not-present, between eCommerce and instore, are blurring. Digital payments don't exist in a vacuum, and fraudsters are exploiting the increasingly complex buying journeys omnichannel retail offers.

For instance, ever faster fulfilment methods such as 'click and collect' offer fraudsters the chance to place an order, pay for it and pick it up in an hour, leaving many merchants struggling to screen their transactions quickly enough to spot fraud. This type of transaction is technically CNP because, even though the fraudster will collect the item instore, the order is placed online. It's a problem for merchants because the liability technically rests with the merchant and not the card issuer, which makes this emergent type of fraud an urgent priority to tackle.

Instore payments are also starting to look very different for many merchants. In addition to the growing support for contactless, many merchants are now also offering alternative ways to pay instore outside of the traditional POS.

Earlier in this section we referenced the fact that instore fraud presents a risk to the fraudster as they are physically present. But as unmanned kiosks and self-scan technology experience mainstream adoption, this concern is mitigated. Remember that criminals have been prepared to carry out their activities face-to-face for thousands of years – today they can use mobile payments, QR payment codes, staffless stores and other emerging payment methods to fraudulently obtain goods quickly and without confrontation. A mark is still a mark.



The Ingenico Perspective

A journey to the Dark Web

The Dark Web hosts a staggering amount of stolen personal and financial information. My first visit felt like a guided safari through the 1990s internet. However, get through the dense thickets and dead-end tracks, and you arrive at one of the many markets. I can buy login credentials to a £30,000 bank account for £300. I can get £5,000 in counterfeit £20 notes for £500. Perhaps the most worrying vista was the site selling 2.1 million stolen PayPal accounts.

As I learnt more, I realised that I can buy credit card numbers, complete with CVV, expiration dates and postal codes for less than £5 each. And I can filter, sort and compare them to find exactly what I want.

Keep digging and you find sites and tutorials offering advice on instore pickup scams, distraction techniques, and insight on 'counter-counter' fraud techniques – how to counterfeit receipts and the best pitch to get a sales assistant to use a damaged or defaced card. The notable difference is the price of wisdom – particularly for instore fraud. Comprehensive and up-to-date instruction on how to effectively target vulnerabilities – particularly instore – costs top-dollar.

The learning from these journeys is that, while compromised data is ubiquitous, the day-to-day understanding of how to use it isn't. Merchants who build defences against fraudulent returns, don't accept physically damaged cards, and train their staff on how to spot and respond to pressure or deception tactics, are in a strong position to protect themselves, their customers and the rest of us.

Adam Roberts
Head of Marketing Communications - Ingenico Banks & Acquirers, EMEA

The Path of Card Fraud

Stage 1: Stealing Card Details

An attacker identifies a weak point in a target environment, then uses one of a variety of techniques to steal card details:

Key logging – Software that records keystrokes made on a computer

Phishing – Disguising oneself as a trustworthy entity via online communication

Vulnerability exploitation – Taking advantage of weaknesses in a retailer's system

POS memory scraping malware – Scanning the memory of POS devices to collect data stored

Stage 2: Selling Card Details

Card details are 'dumped' on the Dark Web to be bought by other fraudsters, often using a cryptocurrency like Bitcoin. These websites include:

Carding Forums - Dedicated websites for selling debit and credit card data

Stage 3: Counterfeiting cards

After purchasing card details, fraudsters convert them into plastic cards using:

Plain plastic cards / Fake counterfeit cards

Magnetic card reader/writer

Specialist software

Stage 4: Using counterfeit cards in scams

Three groups of fraudsters use the counterfeit cards in a variety of scams:

Runners – Individuals that make as many withdrawals on fake cards as possible in a short time span

Droppers – Individuals that take up a temporary residence to receive fraudulently ordered goods

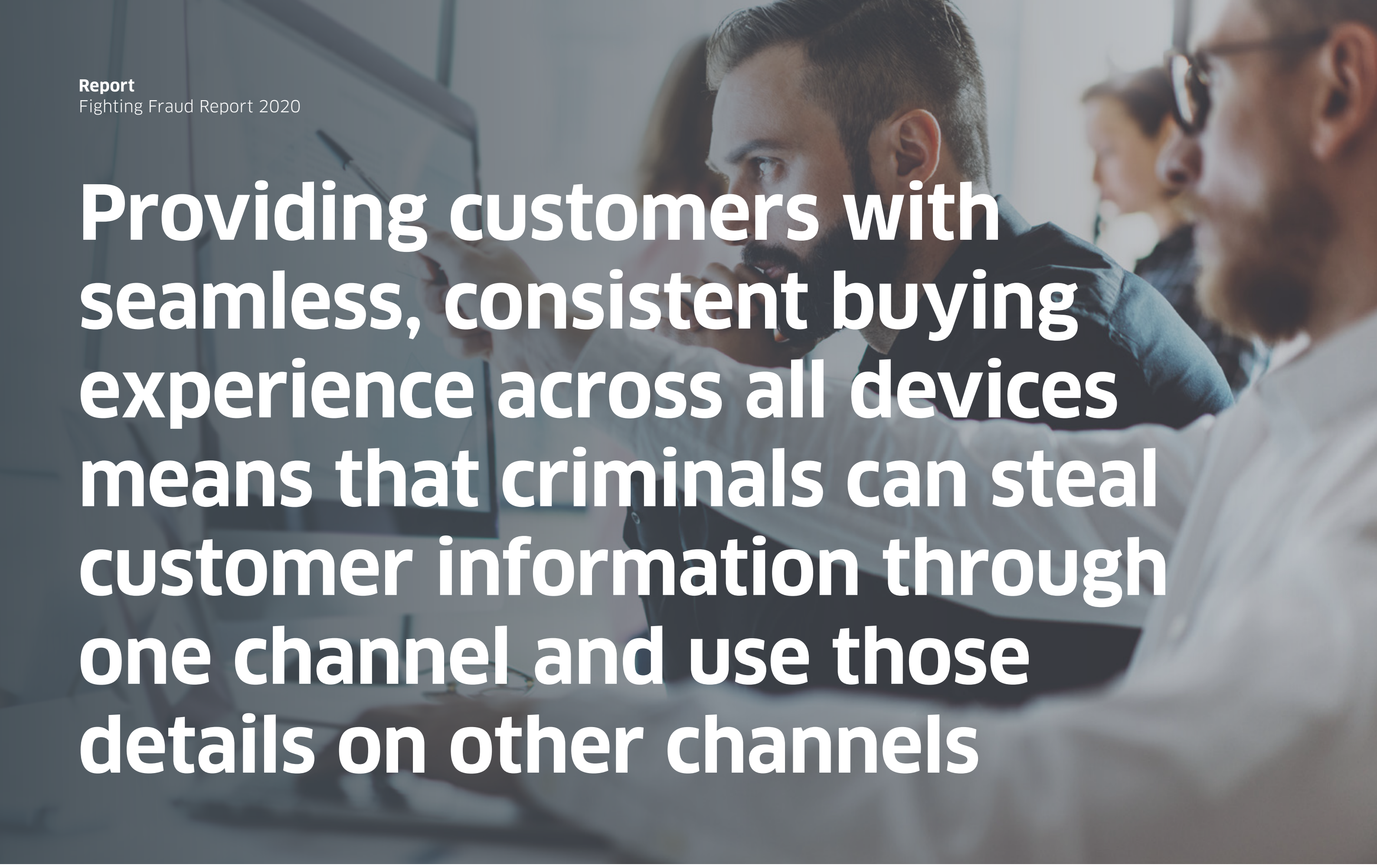
Shoppers – Individuals that specialise in making instore purchases with fake cards

What is the Dark Web?

The Dark Web is part of the internet consisting of encrypted websites essentially invisible to search engines. Users must access the Dark Web through anonymising browsers like Tor that route traffic through worldwide networks of relays to hide the user's location and browsing.

Because browsing activity is near-impossible to trace to the individual, the Dark Web has become a hotbed of criminal activity, including illegal marketplaces to buy and sell drugs, weapons and hacked financial data. Transactions are typically made using cryptocurrencies in order to provide anonymity to the buyer and seller.

After many high-profile data breaches in recent years, people have become less forgiving towards businesses that fail to protect customer information. The scale of the fraud threat now means that many businesses – particularly smaller businesses relying on reputation to attract customers – cannot afford to not take fraud seriously.



Providing customers with seamless, consistent buying experience across all devices means that criminals can steal customer information through one channel and use those details on other channels

4: Enhancing payment security

Just as fraudsters never sit still, the payments industry is engaged in an ongoing struggle to leverage new technologies and techniques before the criminals do. There are many pieces to this puzzle, and while technological solutions are crucial, this challenge cannot be tackled by machines alone. Legislative measures are important, and training and processes must be implemented to counteract the human factor – often the weakest link in fraud prevention. In this section, we will discuss how advances in these areas can better deter, detect and catch payment fraud in the future.

Technology solutions

Artificial Intelligence (AI) and Machine Learning (ML)

AI technology has become so sophisticated and commonplace that it now forms the cornerstone of online fraud prevention and detection. Using rules and predictive models, AI can automatically spot fraud attempts much faster than manual processes, leading to quicker, more accurate fraud decisions.

To keep up to date with increasingly sophisticated fraud attempts, Machine Learning algorithms are fed enormous transaction datasets to uncover and understand evolving fraud methods. This can be split into two categories: supervised ML, in which algorithms are used to map the relationship between input and output variables, and unsupervised ML, in which algorithms model the underlying distribution of data inputs.

These various methods of fraud analysis can be combined to provide a single risk score, generated in fractions of a second, which means that this method can scale to organisations dealing with millions of transactions every day.

However, we live in a world where data-sets are increasingly being leveraged for multiple purposes. There is a greater focus on analysing transaction data for competitive advantage. Counter-fraud is presumably the priority, but is it the only one? And how do we determine the extent to which AI and ML play a part in those various – one could say competing – priorities? The industry is playing catch up with how to regulate the decisions made about – and by – Artificial Intelligence, but the ethics of these questions will become a hot topic in the coming years.

Point-to-point encryption (P2PE)

We live in an era of omnichannel retail, which means that customers interact with retailers over a variety of channels. They may make a CNP purchase on the eCommerce website one day, buy instore with their card another day, or buy instore with a mobile wallet using their phone the next.

However, the drive towards providing customers with seamless, consistent buying experiences across all devices means that criminals can steal customer information through one channel and use those details to make fraudulent purchases through other channels. So, for example, a criminal could steal a card from a customer instore and then use it to make a purchase online. Or a cardholder's information could be stolen from their phone on a poorly secured public Wi-Fi network, and then used to make click-and-collect purchases.

P2PE technology encrypts card data at the point of entry – i.e. a payment terminal or eCommerce checkout page – and keeps it protected until it is decrypted at a secure end point outside of the merchant's environment, usually in the data centres of the merchant's PSP.

P2PE solutions put the merchant's infrastructure 'out of scope', removing the need for them to run complex and costly PCI DSS audits of instore networks, while still meeting the highest level of security when processing card payments. It decreases the merchant's vulnerability to cyberattacks and protects their brand reputation. For acquirers, it adds an extra level of security to card transactions, limiting their exposure to risk. And, for customers, P2PE means that they can continue to have a seamless payment experience across all touchpoints, and no friction is added to the payment process.

Alternative Payment Methods (APM)

As we have alluded to at various points in this report, the growing fragmentation and complexity of the payments ecosystem creates new opportunities for fraudsters. Case in point: APMs, which are currently experiencing an explosion in popularity. Part of the fraud threat that APMs present is that the term covers a variety of disparate methods, from peer-to-peer (P2P) payments to digital wallets to cryptocurrencies.

Consumers and merchants are increasingly adopting payment through digital wallets, specifically mobile wallets like Apple Pay, Google Pay and Samsung Pay, scheme-operated apps such as Masterpass by Mastercard and Visa Pay, as well as localised solutions like iDEAL in the Netherlands.

However, the relative infancy of many APMs means that they are an enticing target for fraudsters. Entrants into the APM market will be more focused on building a customer base and removing friction from the customer experience – which often runs contrary to fraud prevention measures.

As a result, increasingly sophisticated Know Your Customer (KYC) and Know Your Customer's Customer (KYCC) solutions have to be employed to prevent fraud and money laundering through these payment methods.

Biometric authentication

The use of biometric authentication methods is becoming increasingly popular in retail, particularly for physical instore environments. The idea is that physical traits the customer possesses – fingerprints, irises, facial structure, voice - are extremely difficult, if not impossible, to co-opt fraudulently.

The increase in biometric fraud prevention measures has come about largely through consumer devices. Fingerprinting and facial recognition have been popularised by recent iPhone models with thumbprinting and FaceID, and a large range of smartphone devices now incorporate some kind of biometric sensor. Many banking and payment apps now allow users to authenticate payments through a selfie or voice recognition.

Instore retailers can implement biometric devices to guard against fraudulent card present transactions, particularly where the fraudster has managed to acquire the cardholder's PIN number. However, the threat with biometrics is that the technology isn't fast enough for high-volume transactions. Any transaction type that relies on a minimal transaction time – for example, accessing public transportation – is at this point in time unfeasible from a logistical perspective. Although, as the technology improves, we may see much swifter fraud prevention implementations.

Expert Opinion

Defeating fraud shouldn't come at the expense of a retailer's customers

Retailers bristle at the thought of anti-fraud measures adding friction to the customer experience. Speed and convenience are two of the things that keep retailers competitive, so they want to protect them. What's the point of stopping fraud if it drives customers away?

The fight against fraudsters doesn't happen in a vacuum. There are some incredible innovations in anti-fraud technology, but as an industry we need to make sure they meet all the needs of retailers. A revolutionary new measure that loses a business all its sales will struggle to find widespread adoption.

Angela Yore
Co-founder and Managing Director - SkyParlour

Commentary: Amazon Go Stores – A model for the future?

One way in which we can see how instore fraud could be combatted in the future is through Amazon's Go Stores. These stores deliver a 'Just Walk Out' experience in which customers take items and leave the store without interacting with a cashier or payment terminal.

The customer downloads the Amazon Go app onto their smartphone and scans the barcode on the device at the entrance of the store. From that point, a combination of cameras, sensors and Machine Learning identify the customer in relation to their Amazon account. Whenever the customer takes an item off the shelves, it is recorded and charged to their Amazon account.

It is not difficult to imagine how this use of technology in a retail environment could be used to combat fraud. Cameras could passively perform facial scans of customers so that they could be easily verified upon checkout. If the customer's basket is automatically recorded, AI could scan the items to check for any discrepancies that would indicate fraud. And if a customer's shopping experience is inextricably tied to the account they hold with the retailer, then that should reduce instances of card-present fraud.

However, that does not mean that the Amazon Go model is fool proof. Criminals adapt. The main risk is of fraudsters creating a new Amazon account with stolen card details and using that to make purchases instore. Not to mention the possibility for good, old fashioned shoplifting. As fraudsters work out new techniques to exploit the weaknesses of the Amazon Go model, new security solutions (for example, biometric gait analysis) will need to be employed to secure it.

It's probably too early to say whether Amazon Go Stores represent the future of retail or the next evolution in fraud prevention. But there are interesting ideas on show that could be taken up by the wider industry.

Expert Opinion

Data and identifiers will become the fraudsters' next big weapons

The landscape of fraud and fraud prevention is very much a roller coaster – technology advances then new patterns emerge. In recent years, we have seen almost constant waves of development in terms of security advances and regulatory requirements. With technology, we are seeing increasing use of biometrics, including behavioural, and greater adoption of contactless payments. From a regulatory stand point, we are seeing heavily increased security with Secure Customer Authentication, and the advent of 3DS version 2 should provide even greater customer protection over the next year. We are also at the very beginning of what Open Banking can mean for payments.

Where will all these changes lead the fraudster to look next? The trends seem to indicate a move towards the use of data and identifiers. The increasing use of big data in commerce has come with greater customer data vulnerabilities, and fraudsters could look beyond cards, or particular payment types, to make use of account data and identifiers.

David Parker
Polymath Consulting

Legislative measures

PSD2

One of the most important and far-reaching pieces of regulation is the European Union Second Payment Services Directive (PSD2), which aims to regulate payment services in the European Economic Area (EEA).

PSD2 mandated an Open Banking framework for the European payments industry, requiring banking institutions to make their customer financial data available through open application programming interfaces (APIs) to third parties authorised by the customer. Through this framework, previously unregulated companies were brought under the remit of national financial regulatory bodies (for example, the Financial Conduct Authority in the UK).

PSD2 introduced a number of additional consumer protections against fraud, including a reduction in the amount an individual would be obliged to pay in the event of an unauthorised payment (from €150 to €50), dispute resolution procedures for payment complaints, ring-fencing of funds against pre-authorised card payments, and a legal framework for the right to an unconditional refund during an eight-week period.

PSD2 also mandated the introduction of Strong Customer Authentication (SCA) requirements for any purchases made where either the issuer or acquirer is within the EEA. From 14th September 2019, both CNP and CP transactions require two-factor authentication using information that constitutes either knowledge (card number, CVV), possession (smartphone, hardware token) or inherent characteristic (biometric factors such as fingerprint or facial recognition).

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. Regardless of the size of the business, or the number of transactions it conducts, any organisation that accepts credit or debit cards as a form of payment must do the following:

1. **Build and maintain a secure IT network**, including a configured firewall and other bespoke security parameters.
2. **Protect cardholder data** during storage and transmission through encryption.
3. **Maintain a vulnerability management programme** that secures systems and applications against threats.
4. **Implement strong access control measures** so access to cardholder data is restricted on a need-to-know basis and can be traced to individual users.
5. **Regularly monitor and test networks** to identify security issues and track all access to networks and data.
6. **Maintain an information security policy** that governs organisational processes to data security.

Enhanced security solutions work

£2 out of every £3

of attempted fraud was detected and prevented by firms last year.

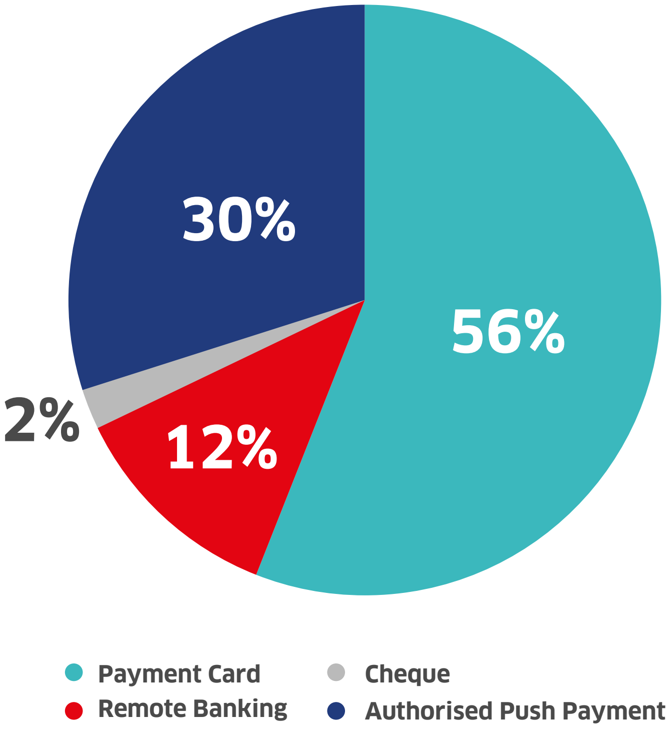
Source: Fraud the Facts 2019

In the past 12 months, security solutions implemented by the finance industry stopped more than £1.6 billion of unauthorised fraud (in which the account holder does not provide authorisation for the payment).

The point is, these innovative measures to protect consumers, in which the industry invests a significant amount of time and resource, do work.

However, we cannot celebrate and congratulate ourselves just yet. Fraudsters are constantly changing their methods, developing new techniques. New forms of fraud will emerge in the coming years that will require new solutions. The fight against fraud is never over, but it's heartening to know that anti-fraud measures can be effective.

Total 2018 financial fraud losses by type



Human error is often the weakest link in the fight against fraud

5: The human element of instore fraud

Most physical payment terminals are designed from the ground-up to be hardened against electronic fraud. In an instore environment, it's most likely that fraudsters will be successful through the human error of retail staff. As a result, there are a few things that staff can look out for to try and combat against common card-present fraud techniques.

Human error is often the weakest link in the fight against fraud. People are fallible and fraudsters are masters of manipulating human nature for their gain. In some respects, the business drive to deliver an excellent customer experience runs counter to fraud prevention - traditional retail wisdom says the customer is always right, but criminals can exploit this to distract from, or push through, fraudulent activity.

So, while there are numerous technological innovations that are helping to fight fraud, there is an aspect of this problem that cannot be solved with machinery. Staff training is a big part of this puzzle, and instore assistants must be rigorously taught how to balance fraud prevention with delighting customers.

Preventing instore fraud - the basics

Have a robust returns policy

Fraudsters know that legitimate returns are a potential weak spot to be exploited for their gain. Returning stolen merchandise or using a counterfeit receipt are therefore popular methods of returns fraud. A returns policy should ensure that customers require a receipt and the original payment card.

Don't accept damaged cards

If the magnetic stripe of a card doesn't work, or the card cannot be read by a chip reader, then that's a warning a sign. Any card that might force staff to manually enter the card number should be viewed with suspicion. Counterfeit cards will be missing things like the issuer hologram too. When in doubt, contact the issuer; a genuine customer with a legitimately faulty card will not be too upset about being unable to make a purchase.

Validate ID

Ask to see some identification from the cardholder to make sure they are who they say they are. But be sure to implement customer care processes that mean you don't overzealously ID every customer that walks through the door.

Learn to spot pressure tactics

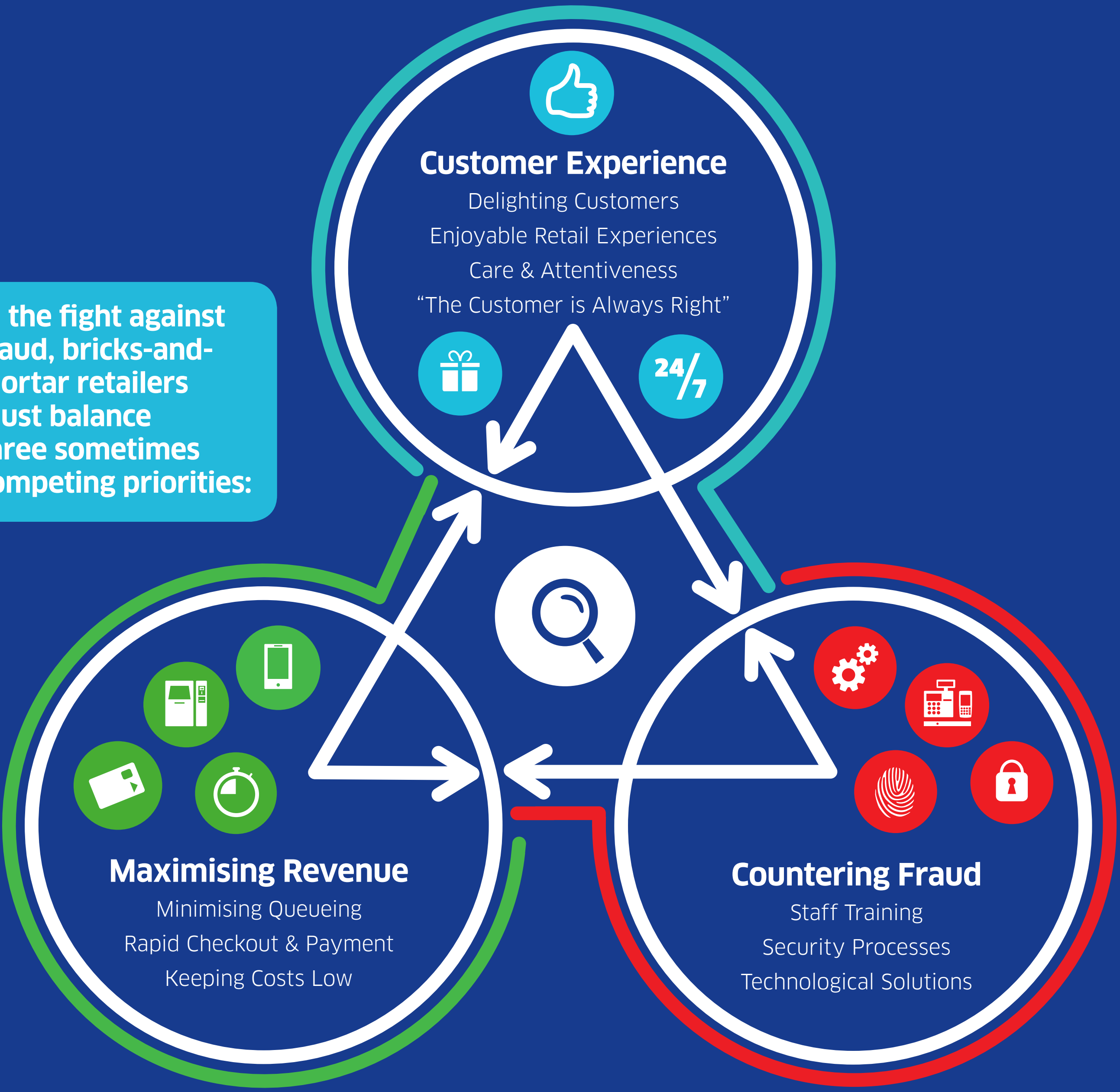
Fraudsters may apply undue pressure – aggression, intimidation, lots of questions, exploit staff willingness to please the customer - to distract from fraudulent behaviour.

Check the shopping cart

If a customer has a large number of products of various prices and styles or even sizes, then they might be wanting to resell the items later. This is a pretty good indication that a stolen card is being used.

Balancing the Fraud Equation

In the fight against fraud, bricks-and-mortar retailers must balance three sometimes competing priorities:



It can seem like prioritising one point on the triangle could come at the expense of the others – you could deliver a great customer service with airtight fraud controls, but you might not be able to do a high sales volume.

However, for retailers, it's not impossible to balance everything. The key is to focus on the human factors – fraud prevention training that teaches sales staff effective processes for spotting fraud, but empowers them to make insightful, pragmatic decisions.

The individual cost of fraud

We can talk about fraud in abstract terms, but what does it really mean for the businesses involved?

Recently, a form of terminal fraud known as 'distraction fraud' has been affecting business all over the UK. The scam involves one person distracting a member of staff while another person hacks a payment terminal to refund themselves a large amount of money on their card.

In one Scottish city, distraction fraud scams have collectively cost local businesses tens of thousands of pounds. One case in the south of England saw a café proprietor defrauded of thousands of pounds by a fraudster pretending to pay for a coffee while an accomplice asked about menu options.

This only strengthens the case for training and education about how to spot fraud attempts. By password protecting payment terminals, keeping terminals in sight of staff at all times, and staying vigilant for any potential distractions, some of these businesses could have avoided devasting losses.

The Ingenico Perspective

The evolution of instore pick-up scams

Not too long ago, fraudsters would have to visit a store to buy goods using a compromised credit card. More recently, fraudsters have used compromised cards to buy online and then have items shipped to a forwarding address.

This approach is high risk, as fraudsters need to have the goods shipped to a customer, then contact the carrier to have the items held in order to pick them up later.

Very crafty fraudsters would push these deliveries to a different location, or even try to have them delivered to a PO box. However, this approach is complicated and requires a degree of fraud savvy to ensure success.

We are now seeing a new breed of fraudsters, one at ease taking advantage of methods that make life easier for legitimate customers. A good example includes a recent shopping innovation: buy online, pick up instore – or BOPIS, as it is commonly called.

With BOPIS, fraudsters may even be as brazen as to directly purchase an item inside the store using valid information from a legitimate customer and pick it up minutes later as if they were the ones placing the order. This particular type of fraud has major implications for merchants, as it is essentially a CNP transaction in which the goods are delivered directly to the consumer within the store.

While continued advances in EMV technology are driving a consistent decrease of fraud in instore shopping, the rise of omnichannel is muddying the waters between instore and CNP fraud. Merchants who recognise the BOPIS threat are deploying specialised controls, including tracking and analysing risk trends associated with types and speeds of delivery, and high-risk products and categories.

Andy Caulkett
Head of Solutions Outcomes – B&A Ingenico Western Europe

6: Conclusion

Payment fraud is constantly evolving. Fraudsters are organised, well-funded and endlessly inventive. As an industry, we must do everything we can to stay one step ahead, utilising bold, innovative new technology and understanding the human and process-driven factors that could help.

This will require in-depth engagement between every corner of the ecosystem – payments experts, acquirers, schemes and technology providers must all join forces to protect merchants and consumers.

That is the purpose of this document - to start a long-term conversation about how we best fight fraud. By providing ongoing information about the evolution of fraud, as well as the most cutting-edge solutions and techniques for fighting it, we aim to keep fraud at the top of the agenda and champion the cause across the ecosystem.

Through robust discussion and collaboration, we can share knowledge, best practices and techniques for beating the criminals. We can empower merchants to protect their profits, their reputation, as well as the customer relationships and experiences that form the bedrock of their business.

In the coming months, we will be talking to merchants, acquirers, banks, fintechs, paytechs and regtechs to build a complex, multi-dimensional picture of the challenges and issues of fraud. From this, we will create regular reports about the state of the industry, exploring merchants' changing anti-fraud needs and providing practical solutions to their most pressing challenges.

This information will be vital to help merchants ensure their business and customers are protected from fraud, as well as to help payment experts continue to develop their platforms so that they recognise the changing face of fraud well into the future. We're looking forward to sharing more insightful, expert content on this topic in the coming months.

To find out how you can get involved in the conversation, contact:

Adam Roberts
Head of Marketing Communications, EMEA
Adam.Roberts@Ingenico.com

To find out more about payment fraud prevention solutions offered by Ingenico, visit: ingenico.co.uk

Sources

1. "Card Payments Pass 75 Per Cent of Retail Sales Milestone in the UK", British Retail Council..
2. "One in three card payments uses contactless technology", AOL.
3. Fraud the Facts 2019: The Definitive Overview of Payment Industry Fraud, UK Finance.
4. True Cost of Fraud Report 2019, LexisNexis.
5. Omni-Channel Retailing The Demand for Cross-Channel Payment Infrastructure Service, Payments Cards & Mobile.
6. "Visa: EMV Cuts Card-Present Counterfeit Fraud by 80 Pct", PYMENTS.com.
7. Mobile Payments & Fraud Survey 2018, Payments Cards & Mobile.

ingenico
GROUP