A holistic approach to fraud protection

Strong fraud prevention without sacrificing the customer experience

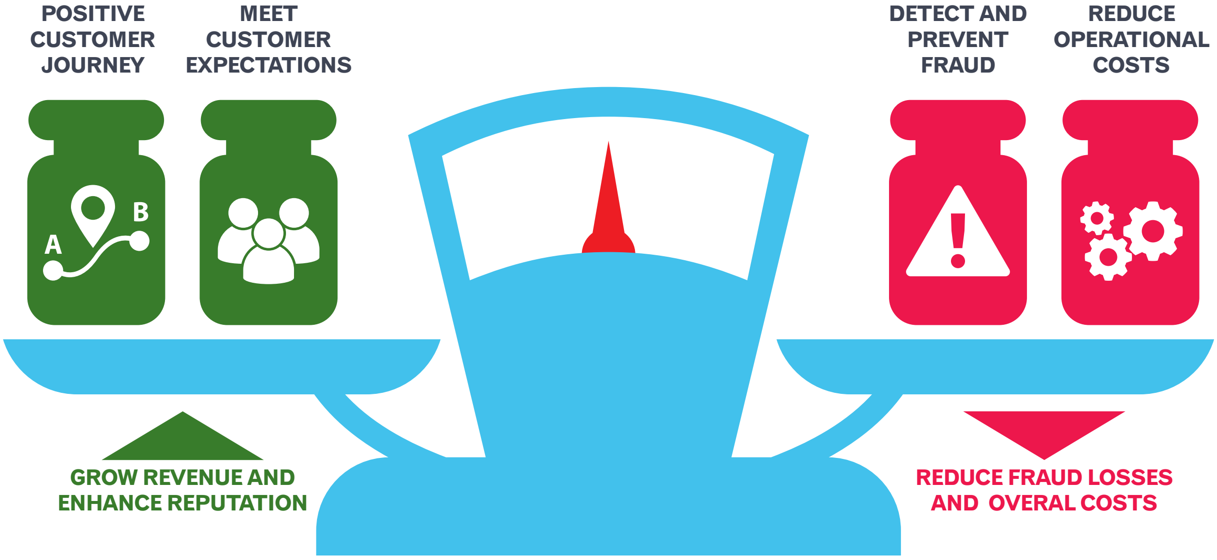
Experian

An Experian white paper

The challenge of balancing competing forces?

Modern, forward-thinking fraud prevention solutions must be highly effective at identifying and preventing fraud, and must do so with as little impact to the customer experience as possible. This was recently reflected in Experian's market research[1], where 71% of financial services and telecoms organisations said protecting the business against fraud at the same time as optimising the customer experience is their top priority over the next five years.

Although many fraud experts believe there is a trade-off between strong security on one side and customer experience and operational costs on the other, it simply is no longer the case. Strong, effective fraud protection can - and should - both enhance customers' experience and lower operational costs. This paper explains why this is true and how to accomplish this goal.


POSITIVE CUSTOMER JOURNEY
MEET CUSTOMER EXPECTATIONS
DETECT AND PREVENT FRAUD
REDUCE OPERATIONAL COSTS
A
B
GROW REVENUE AND ENHANCE REPUTATION
REDUCE FRAUD LOSSES AND OVERAL COSTS

1 - Experian Decisioning Vision 2020 Research (2015) www.decisioningvision.com

The top five trends impacting how organisations assess fraud

1. EMV (or "chip-enabled" cards)

The combination of a "chip and pin" system in credit and debit cards will help prevent counterfeit cards and losses associated with fraud at the point of sale. However, it is widely predicted that organisations will expect to see a sharp rise in card-not-present (CNP) fraud, identity takeover and true-name or synthetic-identity fraud as a result.

2. Online expansion and omnichannel interaction

Mobile commerce has grown by 33%, year-over-year, as of December 2013[2]. As consumers take advantage of organisations offering more products and services online, the potential for fraudulent activity will rise. Customers are now interacting with the same organisation in a growing number of ways, and as more transactions take place in an omnichannel environment, the need for a more strategic and holistic fraud protection strategy is needed.

3. Data breach

With the increase in reported data breaches comes an increased hesitancy from consumers to share their personal information. In addition, as more and more personally identifiable information (PII) is compromised, it becomes less valuable for organisations to use PII as a singular or isolated means of authenticating consumers. Although elements such as name, address, telephone number, and date of birth are important in compliance-oriented identity checking, they are no longer sufficient on their own for risk-based authentication and assessment.

4. Expanded services

Numerous additional services are now offered where personal or financial information is exchanged online or via mobile applications, such as remote deposits and person-to-person (P2P) payments. This allows tasks and transactions to be conducted online, but exposes organisations to new fraud risks. As mobile transactions continue to grow, so too will the number of available online services, making this channel a fertile breeding ground for fraudsters.

5. Regulatory compliance

There are many fraud compliance requirements changing the way organisations do business. Consumers are wary of providing personally identifiable information because of the risk of compromising these credentials, while lenders are tasked with diligently verifying and authenticating the consumer with limited data. Whether it is the European Payments Directive, or anti-money laundering (AML) regulations, levels of assurance in authentication, or a myriad of other guidelines and rules, there exists a tension between meeting such requirements and minimising reliance on personally identifiable information.

2 - Study conducted by Experian

The rise of online fraud and implications on customer experience

Fraud risk has been, and will continue to be, a primary issue for organisations as they strive to be stewards of customer identity and behavioural data associated with customer accounts and interactions. But the more significant issue is the impact fraud can have on the customer relationship. Although the monetary cost of fraud losses can be high, the impact on customer *relationships* can be even higher.

Customers like feeling secure; however they love convenience. And as more and more people start to use convenient digital and mobile channels to manage their finances and do their shopping, the risk of cybercrime rises. In addition, cybercrime techniques are improving and becoming harder to detect and prevent. After all, the internet was never designed to be secure!

Of the top 25 most popular apps, 18 of them failed a security test that was given by McAfee Labs™ in January (2015). Often, the first priority of app creators is to produce the next winning app before their competitors do. Hence, how secure it is isn't the main concern – this explains why there's such a pervasive problem with security in the mobile app world.

Where apps fail to set up secure connections, the opportunity is created for cybercriminals to snatch personal information, such as credit card numbers and passwords. And it's a growing problem because of the ease with which cybercriminals can purchase toolkits that help them infect smartphones via these vulnerable apps.

Organisations in turn are implementing more controls in the hope of mitigating current and impending threats. Sometimes these controls reduce the risk of attacks, yet almost always they degrade the customer's experience by inserting additional barriers.

It's clear that online fraud is increasingly a major concern for businesses around the globe and a clear threat to profitability and consumer trust. Personal data has never been more at risk and easy to obtain for criminals, which will facilitate an increase in identity fraud, leading to increased levels of application fraud and account hijacking.

Whilst the rise of digital business has provided a rich landscape for businesses to interact with their customers in new and exciting ways, it also provides a much simpler way for criminals to attack businesses. Fraud can now be perpetrated on an industrial scale from anywhere in the world, making the job of prevention and investigation much more complex than ever before.

36% of customers are interacting with a single business in five or more channels

85% of consumers use online and mobile to conduct business

Experian Marketing Services research 2015

Why customer experience matters and the impact of intrusive security

Currently, many organisations are experiencing a key challenge; either stronger fraud security is providing a weaker customer experience, or weaker fraud security is resulting in a better customer experience at the expense of increased losses.

However, innovation is on the rise and strong fraud protection can now be achieved **without** sacrificing the customer experience. The latest fraud fighting technologies are keenly focused on identifying fraud attacks, without disrupting the experience of genuine customers. By using cutting-edge technology, combined with behavioural data, organisations are able to provide the positive digital experience customers require, at the same time as identifying criminal attacks quickly and without disruption to the vast majority of good customers.

However, many of the organisations we speak to have found themselves in a difficult situation. The sales and marketing teams have delivered new and innovative ways to transform their business into a digital organisation, but then find that the increase in fraud exposure leads to increased levels of security that can seriously impact the customer experience.

Providing exceptional, seamless service to customers is critical, as 80% of organisations across EMEA say customer experience will be the ultimate differentiator in five years' time. Unfortunately, the imprecise, antiquated fraud controls that many organisations use degrade the service, which is counterproductive to their business goals. Financial organisations struggle with balancing requirements for fraud mitigation and compliance while improving customers' online experience and their own profitability. Additionally, fraud management platforms are simply not keeping pace with evolving, sophisticated fraud methods. These organisations will continue to suffer substantial losses to fraud because cybercriminals frequently find a way around the fraud detection technologies in place.

As consumers we expect great service and the use of intrusive security measures can tarnish our experience and stop us from beginning a relationship with a business, dropping out during the sales process, or even switching to another provider who can offer the digital experience we are looking for. At Experian, our clients are looking to us to help them both reduce the risk of fraud loss to their organisation, at the same time as increasing the volumes of applications that can be accepted, and also protecting the customer experience to ensure retention.

By combining technologies, such as device intelligence and behavioural analytics, businesses can enable customers to interact without the need for 'visible' security, unless the transaction type demands extra levels of security which protect the business and also provide assurance to the customer that their interests are being protected.

The rise of regulation

The European Payments Services Directive (PSD, Directive 2007/64/EC), was introduced in 2007 and adopted into national law around 2009. It defines the legal and technical framework of a common European payments market, in the context of free movement of goods, services and capital.

A further development of the Directive, the PSD2, was proposed by the European Commission in 2013 in order to meet the challenges of the evolving technology since the introduction of PSD, and is expected to be adopted as national legislation as late as in 2017.

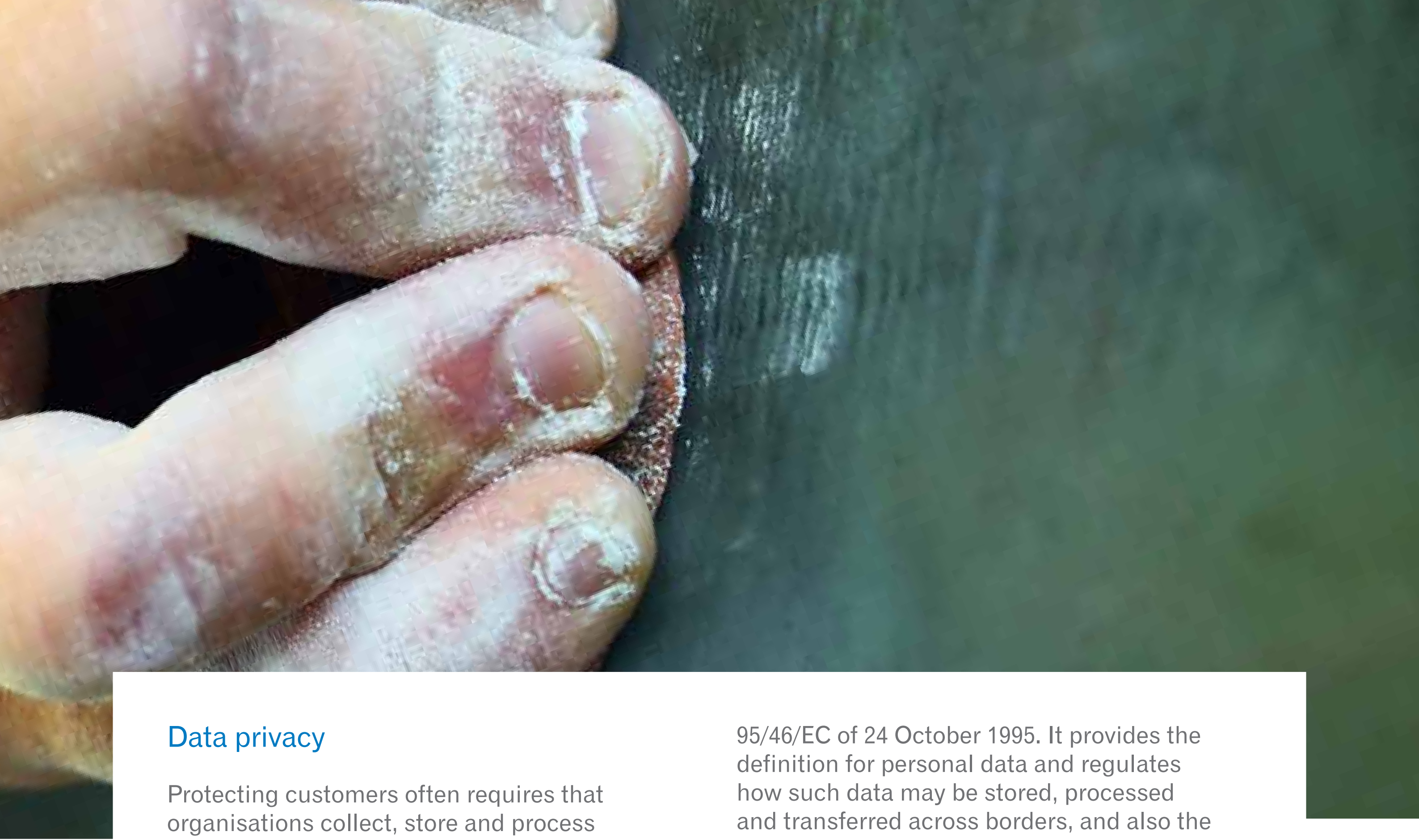
PSD2 focuses on several key areas:

- Providing access to payment accounts to third parties conducting payments business
- Detailing consumer and payment services provider's liabilities in cases of unauthorised payments
- Making payments and charges more transparent and, most importantly from a fraud prevention point of view
- Making strong customer authentication for online payments mandatory

The Commission's definition of strong authentication can largely be interpreted as two-factor authentication. Payment services providers who fail to provide strong authentication will have to indemnify payers from any liability and compensate any losses unless the payer has acted fraudulently. It is unclear if this is going to deliver additional benefits to the consumers already protected by the other liability provisions, or to just contribute to the complexity of the payments IT landscape.

The new European Online Payments Regulations apply to any organisation that touches consumer card data, including banks, merchants, credit card processors, hosting providers, and other organisations that store, process or transmit payment card data. Failure to comply with the requirements may have economic impacts for both merchants and financial institutions.

The biggest takeaway from these new regulations is that there is no one single way to stop online payment fraud. A 'defence in depth' protection strategy, covering all critical areas of the transactional process is the best way to provide consistent and comprehensive fraud prevention. As cyber criminals are innovating and adapting to singular or one-dimensional security systems, banking institutions and merchants need to take a **holistic approach to security** and protecting their customers.



Data privacy

Protecting customers often requires that organisations collect, store and process sometimes large amounts of their personal information. A key assumption in online fraud protection is that any personal information and credentials can be obtained illegally, thus allowing fraudsters to access the accounts of unsuspecting individuals and commit financial crime relatively easily. The ever-increasing amount of information that is required in order to deliver goods and services, but also to protect customers' identities – ranging from basic information to very detailed personal and behavioural data – creates even more comprehensive profiles, and presents ever more lucrative targets for identity theft. On the other hand, any information about the customer is invaluable too in the hands of those who combat fraud.

The requirement to protect the customers' personal details while being able to process, share and use those for the purposes of crime prevention poses additional challenges for both the financial institutions and the organisations specialising in combating fraud.

Designed to protect the privacy, safety and the human rights of the individual, data protection regulations have direct impact on fraud prevention. While relatively clear and centralised in the European Economic Area (EEA), the picture becomes a lot more blurred in other parts of the wider EMEA region.

Personal data processing in the European Union is governed by the European Directive 95/46/EC of 24 October 1995. It provides the definition for personal data and regulates how such data may be stored, processed and transferred across borders, and also the responsibilities of those who store and process personal data.

The picture outside the EAA increases in complexity. While some countries, such as the Russian Federation, have data protection regulations in place, the definitions are different from those adopted in the EAA. A change to the Russian Data Protection Act that limits the handling and storage of personal data of Russian citizens to Russian territory is anticipated to come into force in 2015.

Apart from a few exceptions, countries in other parts of the region, mainly in the Middle East and Africa, have few or no defined data privacy regulations. This creates additional routes and opportunities for financial crime, and delivers new challenges in combating fraud on an international level in the region.

How to implement holistic fraud protection without sacrificing the customer experience

Keeping data security, and compliance, fraud risk, and customer experience at the centre of the authentication equation calls for a need to integrate multiple authentication tools in a layered and risk-based approach to deliver a holistic view of the customer throughout his or her life cycle.

This holistic view will involve the use of advanced analytics and decisioning to validate and authenticate a consumer comprehensively, using multiple data sources, including:

- The data knowingly provided by the consumer
- Behavioural data on the device and the user provided unwittingly within any interaction
- Consortium data collected from other organisations
- Big data from established third parties

A holistic view evaluates the customer from all points of contact and is an on-going process that evolves as more data is captured. Ideally, it is a process that is seamless, timely and applicable to the consumer, based on his or her risk level.

Device data

One of the most significant factors shaping the next frontier in fraud management is the rapid growth in online and mobile commerce as the preferred method of doing business for many consumers. With more than a third of customers interacting with a single business in five or more channels, and more than 85 per cent of consumers using online or mobile to conduct business, the need for omnichannel fraud prevention has become a fundamental requirement.

These trends make device intelligence as important to the authentication process as traditional personally identifiable information. As a result, the need to integrate device intelligence into the authentication process in order to associate a consumer to a known device and its configuration, is critical. Companies are already beginning to incorporate device intelligence into their authentication strategies. The ability to verify a customer through his or her device has a huge effect on the overall customer experience and not only makes it easier for the customer to do business with you, but also adds an additional layer of validation.

Behavioural data

Understanding how customers behave is another key aspect of a modern fraud prevention strategy. The wealth of data collected during interactions with customers allows understanding of risk-free normal behaviours, where minimal interaction is required to allow a transaction to take place. Once a good understanding of a customer’s behaviour is established and understood, abnormal behaviours become much easier to identify, and appropriate risk measures can be deployed.

In the digital channel, there is also the benefit of rich device intelligence that can be blended with the behavioural data to assess risk even more accurately.

Consortium data

Checking data provided by a customer against established sources of negative information is also invaluable in fighting fraud. If information provided during a customer interaction – i.e. email address, mobile number or postal/Zip Code – can be accurately linked to previous negative behaviour, an otherwise clean transaction can be reassessed as high risk.

Using device intelligence can take this approach to a new level, by gaining insight into how devices behave across a wider ecosystem. This can even be applied to devices showing similar characteristics, widening the net and providing real protection against organised fraud.

Consortia data can also be used to gain insight into **positive behaviours**, which can be a valuable tool in helping good customers transact with you. Credit Bureaus have provided these capabilities for many years, allowing businesses to assess credit risk based on past payment performance. In the digital age, businesses can now also assess trustworthiness based on how devices and their users behave across the wider Internet.

Addressing the fraud risk balance

By using cutting-edge technologies that are able to take advantage of device intelligence, behavioural data and consortia data in real time, businesses can start to really change the way they interact with their customers. For example, where it can be seen that a customer's device has a relationship with their account, there is no negative data associated with the device or PII, and their behaviour is within normal parameters, a transaction can easily be assessed in real time to show it is risk free.

On the other hand, if the behaviour is unusual – i.e. sending funds to a new beneficiary or buying a large value item – and the device intelligence is also not normal for the customer, the business can instantly make a high-risk decision and deploy appropriate authentication strategies. The presence of malware in a device can also cause unnecessary friction for a good customer. Their device may indeed be infected with a virus, but this does not mean that there is any malicious intent in the transaction being carried out. By blending and understanding all data available in the transaction, businesses can focus on **protecting against malice rather than just anomaly**, ensuring as little friction for the good customer as possible.

Conclusion

There are a number of factors contributing towards the evolving fraud landscape. Firstly, fraud schemes will continue to rise in sophistication and criminals will remain focused on how to "beat the system". This places continuous pressure on organisations to adopt new approaches to manage fraud and protect information.

Secondly, consumers will expand their use of web-enabled devices and mobile devices to conduct various forms of business, changing the types and amounts of information provided during the application process and transactions. Lastly, regulatory pressures around protecting and disclosing consumer information will continue to rise in breadth and depth.

All of these factors point to the need for organisations to evolve their authentication and fraud management practices to include both offline and online fraud strategies that can deliver a holistic view of the customer relationship across the customer life cycle.

To manage this holistic view of the customer, the authentication process must shift from a single binary-fraud review to a layered, risk-based and contextual authentication approach that will include comprehensive real-time updates of the consumer. Big data and advanced analytics, consumer alerting and multifactor authentication, device intelligence, biometrics, and the sharing of authenticated and credentialed identities across industries will become more commonplace. The ever-changing fraud environment, alongside data and technology evolution, will further drive organisations towards fewer but more robust and dynamic platforms through which to manage customer risk today and for years to come.

In the new digital world it's easy to forget that the vast majority of transactions are risk free. We live in a constant media storm of malware, cybercriminals and hackers. By using all available data in an intelligent and real-time decision process, businesses can deploy next generation fraud prevention techniques that catch more fraud, limit unnecessary friction and reduce operational costs.

About the author: Chris Thomas

Chris has worked in the fraud prevention industry for over 14 years, specialising in helping organisations in the Financial Services, Insurance, Telecommunications and e-commerce industries protect their businesses from criminal attacks.

During the early 2000's, he helped develop the first internet-based employment screening services for Experian, and subsequently spearheaded the development of ID Verification solutions for Equifax in the UK, helping the financial services industry address the requirement for KYC capabilities to address money laundering.

Following this, he worked with the UK retail industry in designing the first purpose-built data sharing scheme to address the growth in internet-based CNP and goods lost in transit fraud. Most recently, he led an initiative for the UK insurance industry, to help protect large insurers from the rapidly growing problem of cybercrime. He successfully cooperated with the industry and law enforcement to identify and prosecute criminal gangs that are using the online channel to obtain insurance policies used to commit multi-millions of pounds worth of fraud.

Chris is widely recognised as an expert in fighting the ever-growing threat of cyber fraud, and in his current role at Experian he is bringing the latest cyber fraud prevention technologies to organisations across the EMEA region.

Chris is also a European Advisory Board Member of the Merchant Risk Council, the leading global trade association for e-commerce fraud and payments professionals.

Denmark
Lyngbyvej 2
2100 Copenhagen
www.experian.dk

France
Tour Europlaza
20 avenue Andre Prothin
92927 Paris La Defense Cedex
www.experian.fr

Germany
Speditionstraße 1
40221 Düsseldorf
www.experian.de

Italy
Piazza dell'Indipendenza, 11/b
00185 Roma
www.experian.it

Netherlands
Grote Marktstraat 49
2511 BH, Den Haag
Postbus 13128, 2501 EC, Den Haag
www.experian.nl

Norway
Karenlyst Allè 8B, 0278 Oslo
Postboks 5275, Majorstuen
0303 Oslo
www.experian.no

Russia
Krymsky Most
6 Bld., 2 Turchaninov Lane
119034 Moscow
www.experian.ru.com

South Africa
Ballyoaks Office park
35 Ballyclare Drive
2021 Bryanston, Johannesburg
www.experian.co.za

Spain
Calle Príncipe de Vergara, 132
28002 Madrid
www.experian.es

Turkey
River Plaza Buyukdere Cad.
Bahar Sok. No: 13 Kat: 8
34394 Levent
Istanbul
www.experian.com.tr

United Arab Emirates
Dubai Islamic Bank Building 01
Office 102, First Floor
Dubai
PO Box 500175
www.experian.ae

Experian
A world of insight