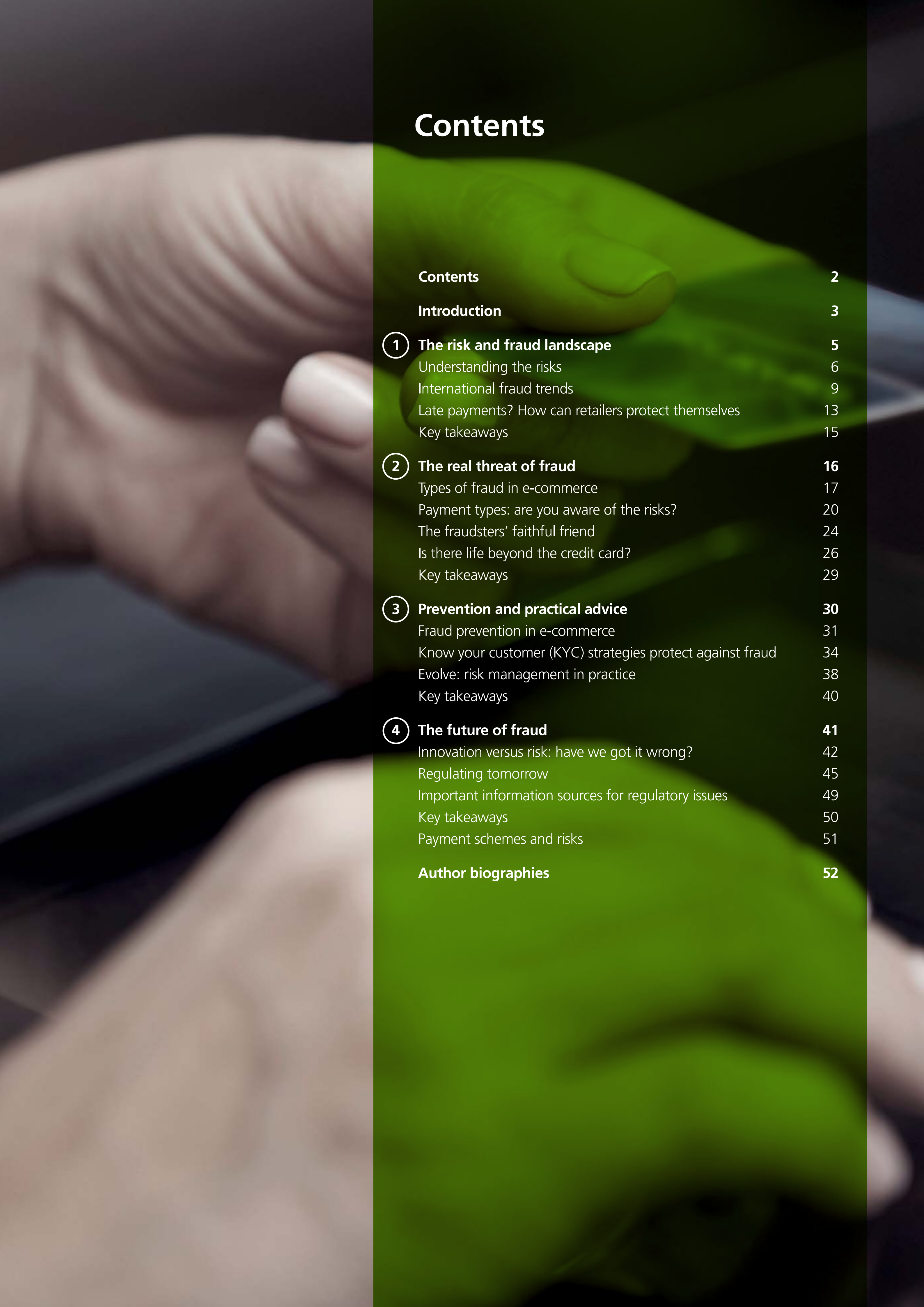
PPRO
the payment professionals

The final frontier –

fighting fraud and reducing risk in international payments



Contents

Introduction

Simon Black, CEO
PPRO Group

As the online payments space enters a period of key innovation and evolution, PSPs have a real balancing act between making sure they speak the language of their ever widening, global customer base and taking advantage of new transaction methods to help their customers remain competitive.

Underpinning all of this – not just for PSPs, but merchants and consumers alike – is the issue of risk and fraud, which poses a very real financial and reputational threat if the dangers are not understood or managed correctly. With new online payment options launching every day and more and more countries opening their doors to international trade, it is an issue that is only set to increase, as merchants continue to develop their global offering.

The issue of risk and fraud poses a very real financial and reputational threat if the dangers are not understood

The payment revolution

From the proliferation of credit and debit card payments through to mobile transactions, e-wallets, biometrics and beyond – the use of physical cash for day-to-day transactions is starting to decline. Indeed figures suggest that cash payments fell from 52 per cent in 2013 to 48 per cent in 2014, and are fast being overtaken by non-cash payments in the UK. The credit card – whilst still popular in the English speaking world – is also set to be resigned to the drawer and used only on rare occasions when needed. Wallets and purses, currently a staple fixture in people's handbags and pockets, will soon serve no purpose and may disappear altogether within the next decade.

In just a few short years from now, payment via smartphone, smartwatches or other intelligent devices is likely to be just as commonplace as paying by cash, debit or credit card today. Be it mobile wallets, virtual cards or biometrics, the world of payments is transforming and cash can expect to slip further down the preference list over the coming years until it will eventually become obsolete by 2025. The end result will enable commerce to be more connected than ever, creating more value and benefits for businesses and consumers alike.

However, with this enhanced value also comes increased risk creating a very real need for merchants and consumers to try and stay one step ahead of the fraudsters, as their techniques also evolve to take advantage of our increased reliance on virtual payment methods.

Fighting fraud

As with all new processes and advances in technology, there are risks. In the case of online payments, the drive towards ease of use could be to the detriment of security, if new methods are not managed in the right way. With more and more value being placed on speed and

PPRO the payment professionals

convenience, consumers are willing to make exceptions and it is this convenience culture that is a major driving force behind the cashless revolution. From using contactless cards to pay for a train journey, to a one-click shop on Amazon, quick and easy is winning the war.

But for all of the convenience, connections and conversions that these new innovations can bring, there can also be a big cost for merchants and consumers. Fighting fraud and safeguarding transactions is still a huge minefield, with each payment process bringing its own risks, from the well established credit card through to the fledgling virtual wallet. Merchants looking to offer new and emerging forms of payment alongside the more traditional options will increasingly look to their PSPs to guide them through the pitfalls and help them put in place appropriate safeguards to ensure the integrity of their transactions and their business.

In this e-Book we aim to provide an overview of the fraud landscape at home and abroad, highlight key threats and trends and provide practical advice for fraud prevention and managing risk, in the midst of an evolving payments environment and increased cross border transactions.

Fighting fraud and safeguarding transactions is still a huge minefield, with each payment process bringing its own risks

Section

1

The risk and fraud landscape

PPRO
the payment professionals

Understanding the risks

Anyone looking to succeed in e-commerce over the next few years must adopt an international outlook. But overseas expansion also brings increased risks.

by Karsten Witke, Head of Payment Services Risk, PPRO Group

M-commerce, omnichannel, business intelligence... the e-commerce industry is a dynamic one, filled with exciting developments. Look away from the hectic, everyday bustle of business, and one strategic development becomes clear: internationalisation. This development has become decisive for almost every online merchant nowadays, and is set to remain so for the next few years. The main attraction of international e-commerce is, of course, enlarging one's target audience, thus increasing revenue and profit. Numerous studies support the opportunities offered by international e-commerce over the next few years, one of the most significant being carried out by OC&C Strategy Consultants[1]. In the world's six largest e-commerce markets alone, cross-border trade will increase more than five-fold by 2020. While, in 2013, this market was worth around 25 billion USD, it is predicted to reach 130 billion in 2020.

Snapshot

- **In the world's six largest e-commerce markets alone, cross-border trade will increase more than five-fold by 2020**
- **Just one in five companies believe that they are well-prepared for new fraud and risk requirements**
- **Working with/using third party partners/ services will provide merchants with a homogenous view of fraud attempts across all countries, channels and payment types**
- **Professional risk assessment is essential, whether it is provided by a merchants own payment service provider or outsourced to others**

Changing markets

Merchants are currently battling three major changes in e-commerce, with the aforementioned internationalisation being the most profound. According to a study[2], however, there are two more: over the next two years, three-quarters of all merchants expect to see a significant increase in mobile transactions, with payment increasingly being made using alternative, local payment methods. As a result, merchants no longer have an overview of the risks involved. As part of doing business internationally, they must familiarise themselves with foreign legal systems, keep an eye on different sales channels, and be capable of estimating the risks involved with (foreign) payment methods. 77 per cent of those surveyed stated that multi-channel payments made it more difficult to detect, deal with, and prevent fraud. The main challenge facing merchants over the next few years is the risk inherent in complex, international e-commerce. According to the study, just one in five companies believe that they are well-prepared for new fraud and risk requirements.

Just one in five companies believe that they are well-prepared for new fraud and risk requirements

Increased risks

International e-commerce should not, therefore, be perceived as a land of milk and honey; after all, increased business opportunities always involve elevated risks and more fraud attempts. Two out of three merchants who took part in the study[2] admitted that they had experienced a noticeable increase in the number of fraud attempts over the past two to three years.

Consumers are failing to adopt high security standards on their mobile devices

Merchants perceive the biggest threats as identity theft, phishing, and account theft, as well as friendly fraud and clean fraud (details are provided in the article on page 17). The merchants surveyed in[2] the study sell to customers in an average of 14 different countries, and this number is set to increase even more over the next few years. Three out of four merchants believe that it will do so over the next two years. Compared to the rest of the world, Europe has very little fraud to deal with. The highest e-commerce fraud rates occur in the USA, followed by India, Canada, Japan and Russia.

Problems with risk management

The current issues with international risk management stem mainly from the inadequate integration of different systems in different countries. As there is no standardised transaction overview, identifying risks is more difficult. Instead, merchants expend much of their resources in using different tools for every single country in which they do business. This unmanageable situation is further exacerbated by the fact that increased sales naturally mean increased transactions, and several merchants make major compromises in risk management out of sheer desperation. One practical approach, for example, involves focusing on minimising risks only in certain countries. That this is more of a stopgap than a genuine strategy becomes clear when you consider further expansion.

Mobile payment risks

One of the greatest risks merchants face involves the increasing number of transactions carried out using mobile platforms, with mobile malware being a primary threat. Spy tools for smartphones and insecure networks (like hotspots) also count as major risks. Additional dangers

Understand both the risks and benefits of offering local (foreign) payment methods

of m-commerce include lost devices, insecure apps, and the users themselves, who don't usually implement the highest security standards on their mobile phones.

The risks of "alternative payment methods"

Credit cards are very susceptible to fraud, but merchants also perceive risks in alternative payment methods. On the one hand, merchants with increasing international exposure must offer more local (foreign) payment methods. Five to six payment types per country are considered the gold standard, and differing preferences within individual countries mean that merchants need to work with 30 to 40 international payment methods. With such a high number of payment types, the administrative effort involved in fraud alone is enormous. Many merchants wrestle with the fact that they no longer have a standardised view of their customers to enable them to estimate risks like non-payment or chargebacks. The other problem is the increased technical challenge involved if, for example, a separate tool is required for each payment type and the data from these tools cannot be meaningfully combined.

Keeping risks under control

International e-commerce creates major opportunities, but it also involves great risks. So what can merchants do? First, they should address the problems they are still battling on a smaller scale. Take, for example, fraud management: merchants should use partners and services which provide them with homogenous views of fraud attempts across all countries, channels and payment types. The same applies to risk management: here, too, merchants need professional solutions to enable them to evaluate their customers accurately from the outset. Merchants also need to realise that professional risk assessment is essential, whether it is provided by their own payment service providers or outsourced to others. After all, very few merchants can afford to (or want to) set up their own dedicated risk management departments.

Notes

[1] www.occstrategy.com/news-and-media/2014/01/global-retail-empire

[2] www.worldpay.com/global/insight-reports/fragmentation-fraud-report

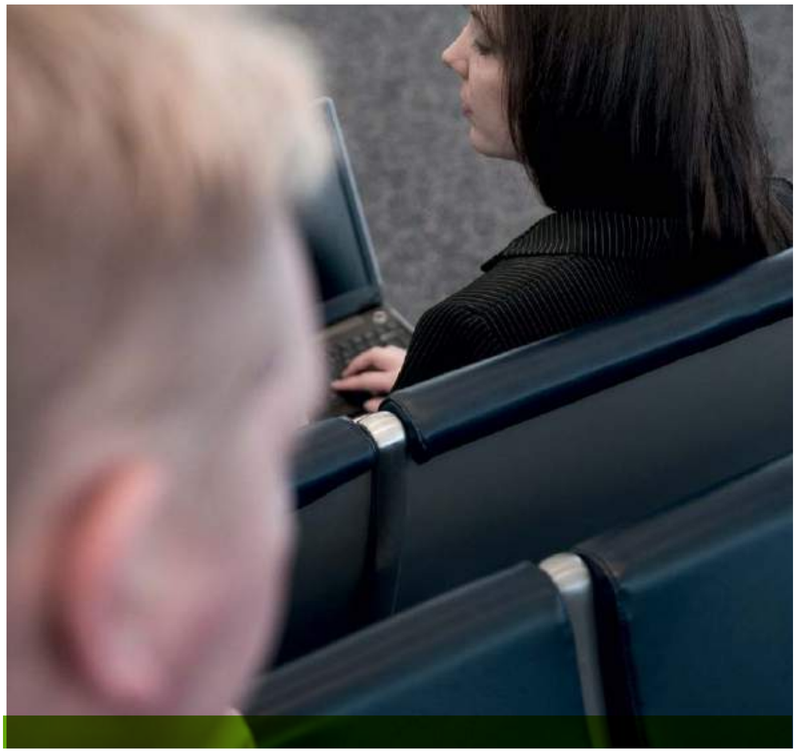
International fraud trends

As e-commerce opportunities continue to develop, so too do fraud strategies. The fraudsters' approaches are multifaceted.

by Andrew Edem,
Head of Engineering & Information Security Officer, PPRO Group

The fraudsters' calculation is simple: where there's a great deal of revenue to be earned, there's a great deal of fraud to be committed. And where there's even more revenue to be earned, there's even more fraud to be committed. In international e-commerce, the signs are pointing the way to increased revenue – and the fraudsters have already muscled in with new techniques.

More online and e-commerce customers equal more victims of fraudsters



Trend 1: E-commerce is an easy target

The more online merchants and e-commerce customers there are, the more potential victims there are for fraudsters. The internationalisation of e-commerce is enabling highly specialised online criminals to become internationally active. Whereas online fraud attacks used to target primarily banks and payment providers, these are now very well equipped to deal with such threats, leveraging technical protection measures and advanced fraud detection services, as well as regulatory standards for the financial industry. Attackers must therefore overcome major obstacles in order to plunder financial institutions. Although online shops tend to be much less well protected, they also process customer data and receive confidential financial information.

The protection mechanisms used by many merchants are not yet state of the art: they do not tend to perform live checks on the customer information entered or deploy sophisticated risk management systems.

Are merchants protecting their customer data?

Trend 2: Identity and account theft

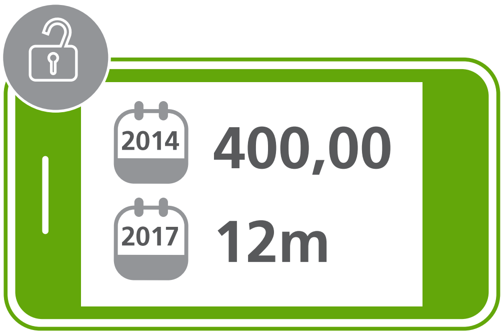
If we look at the methods preferred by cybercriminals, we find that identity theft (often described as "appropriation of identity") and account theft are particularly popular. In identity theft, instead of creating completely new false identities, criminals use stolen personal information as a basis. Account theft, on the other hand, usually involves email addresses and login passwords, which are often siphoned off during hacker attacks on online services. In internet purchase fraud, thieves merely change the shipping address in order to make someone else pay for their purchases.

> ...instead of creating completely new false identities, criminals use stolen personal information as a basis

Trend 3: E-commerce fraud

Mobile is the new desktop. Users are increasingly moving away from traditional PCs and laptops towards smartphones and tablets. The problem here is that protection mechanisms for mobile devices are by no means as comprehensive as those designed for traditional computers. Another oft-neglected factor is that small mobile phone screens make it much easier to stumble upon fraudulent websites – users simply can't see the details as well. Behaviour patterns on mobile devices are different too: smartphone users are accustomed to controlling everything through a few taps, so complex security functions are just not practical. Payment is usually made using one-click methods. Risk management for mobile customers also tends to be problematic, as it is no longer possible to simply evaluate their location – after all, the whole point of mobile devices is to give users freedom of movement. Malware threats on smartphones and tablets also remain an exciting topic. Although it has been talked about for years, experts believe that the great plague of smartphone viruses is yet to come. In 2014, there were around 400,000 new viruses for mobile devices. In 2017, this number is expected to reach 12 million.

...experts believe that the great plague of smartphone viruses is yet to come



Mobile is the new desktop

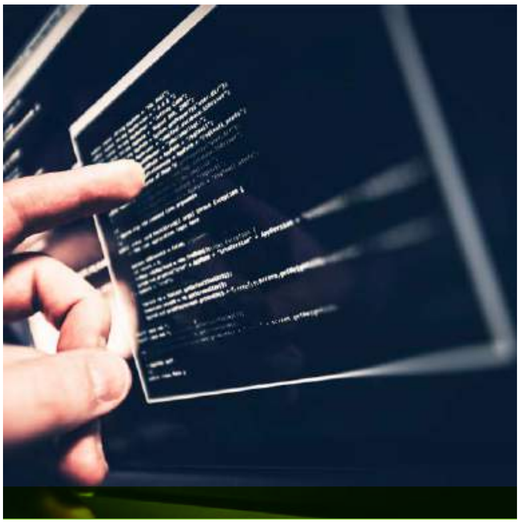
Trend 4: Malware is getting smarter

No matter how comprehensive technical protection becomes, fraudsters use clever malware to keep up. This means that the threats will continue to increase – and not just on mobile devices. All e-commerce channels, whether phone sales or sales via partner platforms, are constantly under fire. The reason for this is that, over the past few years, the malware scene has become extremely professional. As part of its study[1], EMC collected figures relating to online crime. 55 per cent of all attacks on financial data are perpetrated by massive criminal rings. With viruses, however, it is not the sheer number which is terrifying: it is the fact that it is now possible not only to clone viruses, but to modify them in such a way that they form entirely new entities: ones which cannot be detected by existing security mechanisms. Whereas, in 2014, there were around 82 million new viruses a year, there are estimated to be as many as 166 million in 2017[1].

Security cannot be achieved using either a single product or service. Instead, it must be constantly scrutinised and optimised

Trend 5: KYC is not enough

This trend is a result of the aforementioned points. Even if merchants believe they know their customers inside and out, they still need to be cautious. KYC (Know Your Customer) strategies are important, but they are not enough by themselves. Customer classification is a good thing: after all, customers who pay their bills quickly and reliably and bring in large amounts of revenue deserve to choose their payment method. But what if a customer account is hacked? In such cases, it’s not the trusted customer making the purchases, but the fraudster – using the customer’s good name. In addition to the well-known KYC functions, therefore, stores must use fraud detection solutions to recognise when a customer makes unusually frequent purchases or transactions with unusually high totals.



Malware is getting smarter

Putting protection mechanisms in place

As sad as it sounds, there is no such thing as perfect protection. Merchants can, however, use multiple methods to implement effective measures which do not interfere overly with online business:

Multistep security: Security should always be a multistep process. Instead of relying on a single product or strategy, merchants should take a multi-pronged approach, placing particular emphasis on tools and services which can be flexibly adjusted. A behaviour recognition program can, for example, be a valuable enhancement to existing KYC components.

Encryption: As a general rule of thumb, merchants should store only the most necessary data and – if possible – focus on encryption. Of course, data traffic should be transmitted only using encrypted connections.

Learn from your mistakes: As has already been mentioned, there is no such thing as perfect security. But merchants should learn from their mistakes – and from those of others. When it comes to fraud, it helps to deploy a feedback loop which ensures that certain crimes are not repeated. This is how merchants can improve their systems step by step.

Consider security a process: Security cannot be achieved using either a single product or service. Instead, it must be constantly scrutinised and optimised.

Notes

[1] www.emc.com/collateral/analyst-reports/financial-merchants-cyber-threats-aite-102013.pdf

Late payments? How retailers can protect themselves

by Rick Terra
Managing Director, Intrum Justitia, The Netherlands

Small businesses are feeling the strain caused by late payments, but taking some practical steps can reduce the impact. Of all the challenges faced by small business owners, the one that probably causes them the most sleepless nights is late payment from their customers. It's also one of the most common problems encountered in retail. Several governments in Europe recently implemented the "Late Payment Directive" from the European Union. Under these new rules, debtors will be forced to pay interest and reimburse the reasonable recovery costs of the creditor, if they do not pay for goods and services on time (60 days for businesses and 30 days for public authorities). However, it's entirely voluntary and not applicable to business-to-consumer transactions which constitute most of the transactions in retail businesses, and its impact on the problem is debatable. Nevertheless, there are some practical steps that small business owners can take to minimise the impact of late payment.

...a fixed and clear reminder cycle is beneficial for customer retention and gives retail a tremendous boost

Amongst retailers there is a rapidly growing group of companies in the e-commerce market. These companies already use e-invoicing technology and sophisticated payment methods such as PayPal, credit card and mobile wallet applications. The online payment market shows a clear division between no-risk payment methods and payment methods with risk such as credit cards, PayPal, direct debits etc. Payment methods where the customer can pay after receiving their parcel obviously bring a totally different risk to retail. However, the risk is usually carried by the processing partner which charges the merchant a risk fee, usually making this payment method an expensive but a virtually risk-free method for retail.

Late payments are causing sleepless nights

Still, the majority of retailers operate by way of traditional business transactions through "hard copy invoicing" or invoicing by email. Maintaining a good business relationship between the small business owner and their customers is of the utmost importance, in order not to lose these customers to the competition. This does not imply that one can afford to neglect carrying out a continuous check on delayed payments amongst one's customers. Even when all this is done correctly, however, once business owners become caught up in their day-to-day operations, it is easy to forget to send out bills and reminders on time, or to follow up promptly.

Our experience shows that a fixed and clear reminder cycle is beneficial for customer retention and gives retail a tremendous boost. It goes without saying that convincing past clients to purchase again is significantly easier and cheaper than getting new clients.

Sending out courteous reminders by email or traditional post a few days before the invoices are due to clients who have payment terms is advisable.

A reminder stating that the invoice is coming up for payment soon is sometimes all that is needed, especially if the invoice was sent nearly 30 days ago. The sooner you inform your customers that payment will be shortly overdue, the sooner you will obtain payment on time. A persistent and frequent communication with the customer will lead to moderate Days Sales Outstanding (DSO) and thus an improvement of the cash flow situation of the retailer. The reminder cycle should start with a friendly gesture to encourage payment while the second and third reminders can benefit from being a bit more firm. A final date of payment should be quoted as well as the announcement that an additional amount of extra judicial costs will be charged in case one fails to settle an account within a fixed period of time.

A consistent flow of reminder letters next to solid contracts, sales and delivery conditions and invoicing procedures will reduce the problems of late payment. At the same time it's essential that retailers 'know' their new and existing customers by constantly checking the creditworthiness of a company, or, in the case of a business-to-consumer transaction, the private individual. A sensible way to do this is through business information services or via credit checks on consumers. Several state-of-the-art solutions are available to execute automated credit checks merged into scorecards in order to determine low/medium/high risk customers. Scoring methods not only assist the merchant in deciding whether or not a new customer should be accepted but can also be helpful in deciding which dunning processes are the most effective ones. Nowadays, all kind of services are being rendered in order to implement credit rating facilities in the retail accounting system. The customer database will be enriched by customer data and several risk profiles can be developed.

> A consistent flow of reminder letters next to solid contracts, sales and delivery conditions and invoicing procedures will reduce the problems of late payment

However, for retailers for whom cash flow is being impacted by customers who simply don't pay on time, there are still solutions available that can tide them over. For example, if the SME is not willing or able to follow-up his invoicing and past due account procedures, one can decide to outsource part of or the entire credit management service including invoicing, payment service facilities, pre-due calls, in- and outbound calling activities, reminder services etc. It's common practice that these outsourcing activities will be executed in the client's name. If the internal credit management procedures have not led to immediate payment, third party collection services will be invoked. Payment will be enforced by way of amicable means or through legal proceedings, if necessary.

If for some reason a debtor remains in default and no possibilities exist to collect the outstanding account, a debt surveillance service is available regarding private individuals or businesses in certain countries. This third party service will follow up on the debtor's financial situation over the next few years, and take necessary measures to obtain payment in full as soon as it appears that the financial position of the debtor has improved.

For larger companies it may be advisable to consider a debtor purchasing facility in order to obtain cash rapidly. In the business-to-consumer environment, there are a wide range of purchase debt options available.

In high risk portfolios – both international and domestic – where considerable amounts are due, the retailer might consider the possibilities of credit insurance or factoring, although these types of services can be rather costly.

A day-to-day focus on your customer's payment behaviour will certainly pay off and will give a considerable boost to the cash flow position of all companies. As per independent wishes and or needs of the SME one can decide to implement and execute a credit check facility, invoicing and chasing past due accounts, either internally or through a specialised collection agency.

What you should now know

- **Merchants are currently battling three major challenges in e-commerce – internationalisation, mobile transactions and evolving global risk and fraud patterns.**
- **Compared to the rest of the world, Europe has very little fraud to deal with. The highest e-commerce fraud rates occur in the USA, followed by India, Canada, Japan and Russia.**
- **One of the greatest risks merchants face involves the increasing number of transactions carried out using mobile platforms, with mobile malware being a primary threat.**
- **No matter how comprehensive technical protection becomes, fraudsters will use clever malware to keep up. This means that the threats will continue to increase – and not just on mobile devices.**
- **Of all the challenges faced by small business owners, the one that probably causes them the most sleepless nights is late payment from their customers. It's also one of the most common problems encountered in retail.**
- **Even if merchants believe they know their customers inside and out, they still need to be cautious. KYC (Know Your Customer) strategies are important, but they are not enough by themselves.**
- **There are a number of key steps for fighting fraud and managing risk which will not overly interfere with online transactions, including: putting in place multistep security; encrypting information; learning from your mistakes; and seeing security as a process.**

Read on to learn about the real threat of fraud

Section

2

The real threat of fraud

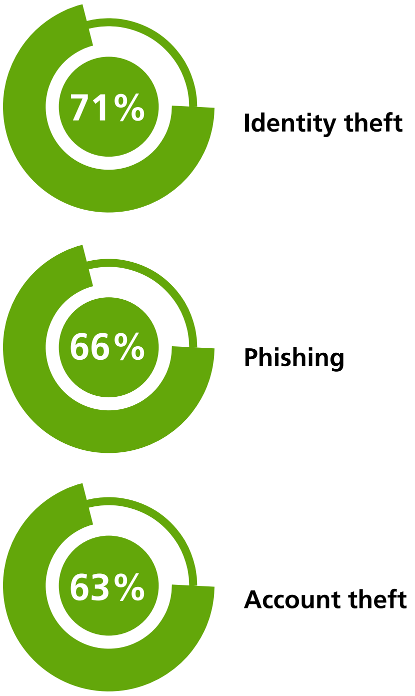
the payment professionals

Types of fraud in e-commerce

Snapshot

- **Internet payment fraud continues to rise, with the number of cases increasing by 19 percent compared to 2013**
- **Over half of merchants have difficulty in maintaining an overview of fraud prevention tools in different countries**
- **Merchants should assess the risks with payment methods to find the perfect payment mix for their online outlet**
- **Fraud involving credit cards has skyrocketed since the e-commerce boom of the 1990's with losses from UK-issued cards in 2014 amounting to £479 million**

...the most common types of fraud causing concern are:



E-commerce revenue is constantly increasing, but the number of fraud cases, as well as the percentage of fraud in online transactions, is increasing faster still. But what types of fraud exist and – more importantly – how can we protect ourselves against them?

by Karsten Witke, Head of Payment Services Risk, PPRO Group

The Nilsen Report[1] uses the example of card-based payments to illustrate the point: Internet payment fraud is constantly increasing, and is, apparently, unstoppable (see page 24, The fraudsters' faithful friend). While the increase itself is nothing new (there has been more e-commerce fraud every year since 1993), the rate is impressive. The number of fraud cases has increased by 19 per cent compared to 2013, and this is the fourth successive time that fraud growth has exceeded e-commerce growth. Out of every 100 USD in turnover, fraudsters currently snatch 5.65 cents.

Fraud is not exclusive to credit card payments, however. Criminals are becoming more sophisticated in their use of malware to command online banking logins via phones, tablets and computers, using the stolen bank account details to make fraudulent payments. "Alternative" payment methods are also attracting criminals. So what does this fraud look like, exactly? A study[2] asked 274 merchants from various industries in six countries precisely this question. The most common types of fraud are explained below.

Identity theft

According to the study[2], the most common types of fraud causing concern among merchants are identity theft (71 per cent), phishing (66 per cent) and account theft (63 per cent). Here, credit cards are the most popular target, as a fraudster does not need much to carry out a "card not present" transaction.

In traditional identity theft, the criminals' goal is to carry out transactions using a different identity. Instead of having to come up with a completely new identity to do this, they simply take over an existing one. This is easier to do – and usually much faster.

In order to commit identity theft or appropriate someone's identity, fraudsters target personal information, such as names, addresses and email addresses, as well as credit card or account information. This enables them, for example, to order items online under a false name and pay using someone else's credit card information or by debiting another person's account. Phishing, on the other hand, simply involves using fraudulent websites, emails or text messages to access personal data. Another technical method is known as pharming, in which manipulated browsers direct unsuspecting customers to fraudulent websites. Often, all that is required to appropriate someone's identity is a stolen password. This can be used to take over an existing account with an online shop – in most cases, the payment data is already stored in the account.

Of course, hacker attacks on e-commerce providers and stealing customer data also fall under this fraud category, as does using malware on computers to commit identity theft by spying out sensitive data. "Man-in-the-middle attacks" are even more sophisticated. These involve hackers muscling in on communications between customers and merchants (or between customers and banks) in order to siphon off login data.

Internet payment fraud is constantly increasing

We haven't even mentioned the opportunities involved in intercepting credit cards sent by mail, for example, or in copying credit cards in restaurants and hotels or at cash machines. Already, though, the true extent of the identity theft problem is apparent.

Friendly fraud

In fourth place is what the merchants surveyed[2] refer to as "friendly fraud". This sounds friendlier than it really is: using this method, customers order goods or services and pay for them – preferably using a "pull" payment method like a credit card or direct debit. Then, however, they deliberately initiate a chargeback, claiming that their credit card or account details were stolen. They are reimbursed – but they keep the goods or services. This fraud method is particularly prevalent with services, such as those in the gambling or adult milieus. Friendly fraud also tends to be combined with re-shipping. This is where criminals who use stolen payment data to pay for their purchases don't want to have them sent to their home addresses. Instead, they use middlemen whose details are used to make the purchases and who then forward the goods.

The true extent of the identity theft problem is apparent

Clean fraud

Clean fraud's name is misleading, because there's nothing clean about it. The basic principle of clean fraud is that a stolen credit card is used to make a purchase, but the transaction is then manipulated in such a way that fraud detection functions are circumvented. Much more know-how is required here than with friendly fraud, where the only goal is to cancel the payment once a purchase has been made. In clean fraud, criminals use sound analyses of the fraud detection systems deployed, plus a great deal of knowledge about the rightful owners of their stolen credit cards. A great deal of correct information is then entered during the payment process so that the fraud detection solution is fooled. Before clean fraud is committed, card testing is often carried out. This involves making cheap test purchases online to check that the stolen credit card data works.

Affiliate fraud

There are two variations of affiliate fraud, both of which have the same aim: to glean more money from an affiliate program by manipulating traffic or signup statistics. This can be done either using a fully automated process or by getting real people to log into merchants' sites using fake accounts. This type of fraud is payment-method-neutral, but extremely widely distributed.

Triangulation fraud

During triangulation fraud, the fraud is carried out via three points. The first is a fake online storefront, which offers high-demand goods at extremely low prices. In most cases, additional bait is added, like the information that the goods will only be shipped immediately if they are paid for using a credit card. The falsified shop collects address and credit card data – this is its only purpose. The second corner of the fraud triangle involves using other stolen credit card data and the name collected to order goods at a real store and ship them to the original customer. The third point in the fraud triangle involves using the stolen credit card data to make additional purchases. The order data and credit card numbers are now almost impossible to connect, so the fraud usually remains undiscovered for a longer period of time, resulting in greater damages.

Merchant fraud

Merchant fraud is another method which must be mentioned. It's very simple: goods are offered at cheap prices, but are never shipped. The payments are, of course, kept. This method of fraud also exists in wholesale. It is not specific to any particular payment method, but this is, of course, where no-chargeback payment methods (most of the push payment types) come into their own.

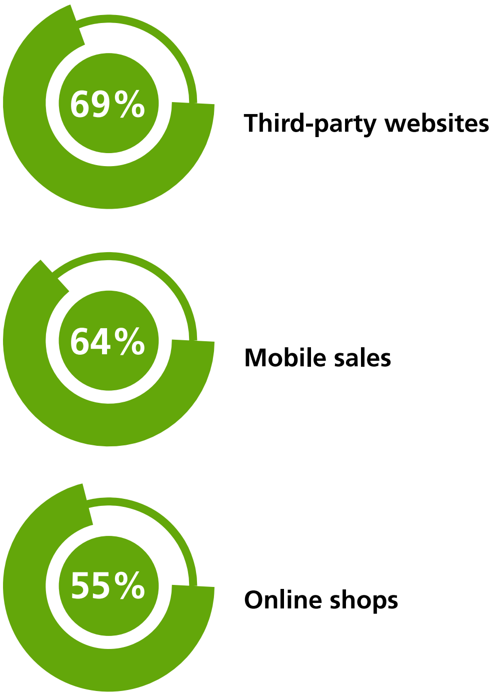
More international fraud

On average, the merchants who participated in the study[2] do business in 14 countries. According to 58 per cent of those surveyed, the major challenge in fraud prevention is a lack of system integration to provide a unified view of all their transactions across all markets. 52 per cent also see increased international transactions as a challenge. Almost exactly the same number (51 per cent) have great difficulty in maintaining an overview of the various fraud prevention tools in different countries. Language barriers, as well as the difficulty of keeping international tabs on individual customers, pose additional fraud management challenges.

Different devices

Fraud methods vary depending on the sales channel, and the fact that most merchants aim to achieve multi-channel sales does not make the situation any easier. According to 69 per cent of the merchants surveyed in[2], sales via third-party websites like Amazon, Alibaba or eBay are particularly susceptible to fraud. These are followed by mobile sales (mentioned by 64 per cent) and sales via their own online shops (55 per cent).

Fraud methods vary depending on the sales channel:



Notes

[1] www.nilsonreport.com/publication_chart_of_the_month.php?1=1&issue=1068

[2] www.worldpay.com/global/insight-reports/fragmentation-fraud-report

Payment types: are you aware of the risks?

From every 100 USD generated in sales, almost 6 US cents are lost to fraud

E-commerce fraud is a problem, but it's not the only one. Merchants should be aware of all the risks associated with the array of payment types available to them.

By Ralf Ohlhausen, Payment Expert and Chief Strategy Officer, PPRO Group

Fraud is fraud – including the theft of PayPal account information and its use for nefarious purposes, such as going on a shopping spree at someone else's expense. The different types of fraud merchants should look out for are described in Types of fraud in e-commerce on page 17. However, to judge a payment type solely by its fraud risk is a mistake and, if everyone did that, no merchant would ever accept credit card payments. SEPA direct debits would also be a no-no, as both payment types are assessed by experts as carrying a high risk of fraud. In practice, however, merchants should assess the risk that comes with each payment method to find the perfect payment mix for their online outlet.

> ...merchants should assess the risk that comes with each payment method to find the perfect payment mix for their online outlet

Guaranteed payments

E-commerce is growing. From every 100 USD generated in sales, almost 6 US cents are lost to fraud (1). How, then, can merchants ensure that they hold onto the remaining 99 dollars and 94 cents? The simple answer is to use payment types with payment guarantees. This is the only way merchants can minimise the risk of payment default. Invoices and credit cards, for example, provide no payment guarantees; nor do SEPA direct debits or immediate transfers. Giropay, on the other hand, guarantees payments, as do EPS, iDEAL, Paysafecard, SafetyPay and Qiwi. As a general rule of thumb, push payments, where the customer initiates the payment, are always more merchant-friendly than pull payments, where the merchant has to "fetch" payments from customers.

The risk of chargebacks

The second most significant risk merchants must weigh up when looking at payment methods is chargebacks or payment reversals, especially with credit cards, although there are major differences between countries. It is, for example, relatively difficult to cancel a credit card payment in Germany, whereas the process in the USA requires just a few clicks of the mouse. SEPA direct debits, on the other hand, can be easily cancelled by customers everywhere, and the chargeback rate is correspondingly high. Many customers who have initiated this type of chargeback point out that reversing the charge was easier for them than contacting the merchant[2].

The consequences of chargebacks

Merchants should also take into account that chargebacks do not only result in customers receiving refunds. They also have many undesirable side effects, often giving rise to a great deal of administrative hassle. To add to this, credit card companies also keep a close eye on the chargeback

> When it comes to credit cards, for example, merchants can easily avoid chargeback fraud by building in additional security functions, like 3D Secure

Credit card companies need to keep a close eye on the chargeback rate

rate. If a merchant accumulates too many chargebacks, they can be fined. Exceeding a particular chargeback limit can even lead to merchants being blacklisted, preventing them from accepting any credit card payments for a certain period of time. This, of course, also damages merchants' businesses, because credit cards have become one of the world's most popular payment methods. Merchants can, however, also take certain measures to minimise fraudulent chargebacks. When it comes to credit cards, for example, they can easily avoid chargeback fraud by building in additional security functions, like 3-D Secure.

It is extremely difficult to commit fraud using any payment type based on online banking processes if up-to-date security measures are deployed

Unnecessary expenses and risks to reputations

One major issue for merchants is that, in practice, problems are often associated with unnecessary costs. This applies, for example, to the aforementioned chargebacks and payment reversals, in which the fees incurred are paid by the merchant. The reputational risk for merchants is usually the result of another risk. If, for example, we take the example of too many credit card chargebacks, acquiring a poor reputation with a credit card issuer can cause lasting damage to a merchant's good name. News of these frequent discrepancies with other payment types will travel fast, especially on social media, meaning customers will soon hear about it, which can further damage a merchant's business.

Failed and late payments

Failed payments can also be triggered by posting errors. The risk is that, although a transaction is confirmed successfully by a particular payment system, the money never arrives. Merchants also incur damages as the goods are usually sent as soon as the payment confirmation is received. There is also increased administrative effort involved, as merchants must first realise that a payment is missing and then trace back the transaction to see exactly what happened. There are instances with certain payment types in which the payments almost never fail, while, for others, 0.5 to 1 per cent of transactions are affected. Merchants' payment goals are often several weeks out, so the money does not necessarily have to reach them immediately. Plus, it can be a problem if late payments mount up.

Notes

[1] www.ilsonreport.com/publication_chart_of_the_month.php?1=1&issue=1068

[2] www.transactionworld.net/articles/2014/april/chargebacks.html

Which payment type has the highest risk of fraud?

Risk of fraud

What is the fraud risk for specific payment types? If we categorise the risks as "high", "medium" and "low", credit cards and SEPA direct debits are the payment types with the highest level of fraud risk. Credit cards and account data can be stolen, and "friendly fraud", the deliberate initiation of chargebacks, is possible with both payment methods. The bulk of payment types, on the other hand, have a low fraud risk. These include giropay, EPS, iDEAL, Paysafecard or SafetyPay. It is extremely difficult to commit fraud using any payment type based on online banking processes if up-to-date security measures are deployed. Even the more vulnerable payment methods, such as credit cards or direct debits, are important elements in the payment mix due to their extreme international popularity.

Minimising risks

Although merchants should be able to estimate the risks involved in accepting different payment types, they are not powerless against them. There are several approaches merchants can take to minimise the risks associated with the various payment types. The article on page 31 highlights the technical options, while risk management is detailed on page 38. The article on page 51 covers knowing your customer.

The fraudsters’ faithful friend

As the most popular payment method after cash, fraud figures involving credit cards have skyrocketed since the e-commerce boom of the 1990’s...

by Ralf Ohlhausen
Payment Expert and Chief Strategy Officer, PPRO Group

Before the birth of the credit card and advent of online shopping, transaction fraud was rare. Fast forward to today and “plastic fraud” is rife and moreover expected by merchants, many of whom skip straight to damage limitation rather than trying to fight it. As the most popular payment method after cash, fraud figures involving credit cards have skyrocketed since the e-commerce boom of the 1990’s with fraud losses from UK-issued cards in 2014 alone, amounting to 739m USD[1]. “Card-not-present” transactions have made it all too easy for fraudsters to bypass crucial, physical control mechanisms including a signature, photo comparisons, or chip-and-PIN processes which simply cannot be carried out online.

Attempts to limit the losses

To limit rising figures, the credit card industry has made various attempts over the past 20 years to stop the fraudsters in their tracks, with varying degrees of success.

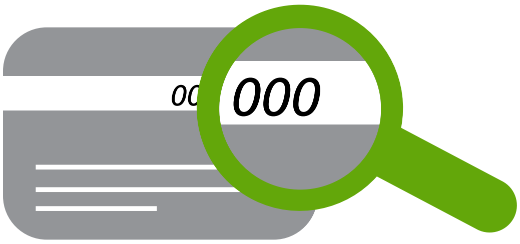
With the introduction of PCI DSS (payment card industry data security standard), merchants were required to implement security measures to secure credit card details that they had stored or collected. A 12-point list details the security requirements for merchants’ IT environments and those of Payment Service Providers and companies that don’t adhere to the requirements, are not permitted to perform credit card transactions. The introduction of the standard has affected mostly smaller merchants, whose lack of PCI certification means that their credit card transactions need to be performed by PSPs or other financial institutions who have the high security standards required. Unfortunately, the introduction of (and adherence to) PCI DSS has not prevented the details of millions of cards from being stolen over the past few years, particularly from major merchants – ironically.

Other approaches to secure online credit card use have involved the card holder needing to provide the expiry date and address details to verify their identity. The latter can, however, only be verified in a few countries and even then, often not completely. In 3-D Secure, the industry thought it had scored its greatest hit. During this payment process, cardholders were redirected to the banks which issued their credit cards and asked to enter a secret code in a pop-up window. This requirement, however, led to customers terminating orders during the final step, either because they had forgotten their code or because they hadn’t registered with 3-D Secure in the first place. Although this option put the liability onto the bank and cardholder rather than the merchant for any fraudulent transactions, it was deemed a conversion killer and as well as reducing fraud it also reduced transactions.

As an alternative method of verification, most sites merely ask their customers to enter the security code (CVC, or Card Validation Code) printed on the back of their card when processing a transaction. As these codes may not be stored by the merchant or by any other partner involved in the transaction, this method provides a certain measure of security for the cardholder but is however useless if the card is stolen or photocopied.

The most recent approach to securing online credit card transactions is known as "tokenisation". In order to carry out this process, credit card companies store a numerical "token" for each credit card in a database. This is then shared with the merchant during the online payment process, rather than sharing the credit card details themselves. The payment is authorised by automatically comparing the token with the credit card company's database. The original idea was to assign a new token for each transaction, but for those merchants offering the popular one-click payment option, static tokens are needed which can be stored and re-used for each payment, which increases the risk once again.

As an alternative method of verification, most sites merely ask their customers to enter the security code



No one-fix solution

The bottom line is that despite numerous efforts to make the credit card a secure method for online payment, they have not had a lasting effect due to a number of reasons, with fraud figures showing no signs of stabilising or decreasing in the short-term.

Criminals will always find loopholes and the processes designed to increase online security are often dismissed by merchants or poorly implemented, due to concerns around the affect upon order conversion rates. When it comes to card payments, there is, unfortunately, no one solution to this dilemma, as payments initiated by merchants which require data to be transmitted or stored in some form will always leave a back door open for data thieves.

The challenge for merchants is to incorporate alternative payment options to help them spread the risk and offer shoppers a more secure method for payment alongside the trusted and much loved credit card, whilst safeguarding their own finances.

Notes

[1] www.theukcardsassociation.org.uk/plastic_fraud_figures/index.asp

Is there life beyond the credit card?

by Andrew Edem
Head of Engineering and Information Security Officer, PPRO Group

In the UK and across the English speaking world, credit card payments remain prominent, totalling £14.6 billion in May 2015 alone. Despite new innovative payment methods on the horizon, the popularity of credit cards as an online payment method shows no signs of diminishing and renewed efforts to fight fraud are not making much of a dent.

> Despite new innovative payment methods on the horizon, the popularity of credit cards as an online payment method shows no signs of diminishing...

For those operating across international online borders, getting to grips with and fighting card fraud can be even more difficult. For example, in Germany, credit card usage for online payments and "card not present" transactions is low, with invoice and SEPA direct debit leading as the more popular options. In the Netherlands, almost two thirds of shoppers use iDEAL which prevents the misuse of sensitive data by putting the onus on the shopper to initiate the payment meaning merchants don't collect it in the first place. In the US, credit card use is prevalent but they are only just undergoing migration from magnetic strip to chip–and-pin so the nature of fraud in this territory will change from cloned cards to "card not present" transactions in the near future.

Credit card payments across the UK and English speaking world totalled £14.6 billion in May 2015

Varying credit card penetration and usage across different territories can make a global response difficult. But with e-commerce an easy target for fraudsters and at best, attempts by the industry to stay one step ahead are still a few years behind, risks of credit card fraud still remain no matter who you are and where in the world you operate.

Hacking of gamer accounts and theft of credit card details is increasing

Assessing the risks

The use of credit cards to make a purchase can be a double edged sword for both merchants and consumers alike. For merchants, credit card payments will increase conversion rates in those territories where usage is high but with that, the likelihood of fraud also increases which could lead to both monetary and reputational consequences.

High profile cases of Sony Playstation, Xbox and Amazon user accounts being hacked and credit card numbers and expiry dates being published, are increasing in occurrence alongside the more common, daily risk of chargebacks. This shows just how vulnerable and valuable customer data is to a fraudster and how companies which rely on credit card payments could be opening themselves up to financial reputational damage.

For larger companies, being able to deal with fraudulent transactions and data theft might not have a significant impact on their bottom line or long-term reputation, but for smaller ones, a fraudulent transaction or data breach could cost them dearly.

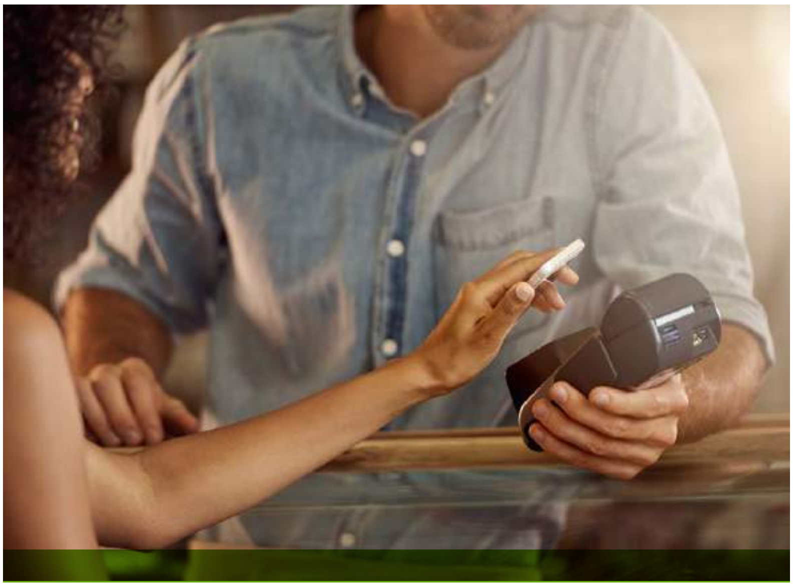
The right response?

We have already discussed security measures and the attempts to minimise fraudulent online transactions, but what steps can merchants realistically take to minimise the impact whilst still ensuring consumers can use credit cards safely and securely?

As a rule, these types of “pull” payments – i.e. those initiated by merchants – are less secure and appropriate for online purchases, with the merchant storing customer data and becoming an easy target for data theft. To try and counteract this risk, the credit card industry has introduced measures including 3-D Secure to authenticate online payments which prompts the card holder to provide a password associated with that card, making them more of a “push” experience. These efforts have however had a largely detrimental effect on transaction rates and as such adoption among merchants is still low.

On top of this, merchants can incur the additional risk of chargebacks. Originally designed to provide security for dissatisfied customers, by enabling them to dispute charges and receive their money back, this concept has established itself as a playground for swindlers. In “friendly fraud”, customers simply maintain that they did not place a particular order, or that they never received their items. In such cases, merchants are almost always left holding the baby.

Credit cards are an integral part of online shopping, but a “healthy mix” is recommended. Online merchants should always offer “push” payment methods as well as including invoicing, prepayment and real-time bank transfer systems and schemes such as giropay and SOFORT banking in Germany, iDEAL in the Netherlands, Przelewy24 in Poland or Boleto Bancario in Brazil, all of which prevent misuse of sensitive data by not collecting it in the first place.



Merchants need to know how to reduce the risks of credit card payments

With push payments there is trade-off between convenience and security

These consumer initiated payments mean the shopper needs the merchant's details but their details remain secure. With push payments fraud is reduced, but there is a trade-off between convenience and a more robust, secure option. For merchants, push methods mean less work, they don't have to adhere to the strict PCI (payment card industry data security standards) rules and the shopper has no chargeback right as they would with a credit card payment. The onus is therefore very much on the consumer to initiate the payment which can require more administration and effort. As a result, push payments could be perceived as an inconvenience for those used to the ease of paying by credit card or one-click ordering.

In addition to considering alternative methods of payment it is important for merchants to know how to reduce the risks associated with credit card payments so they can continue to offer it alongside additional options.

In our experience, there are a number of key steps that merchants can take to minimise the risk of fraudulent card transactions:

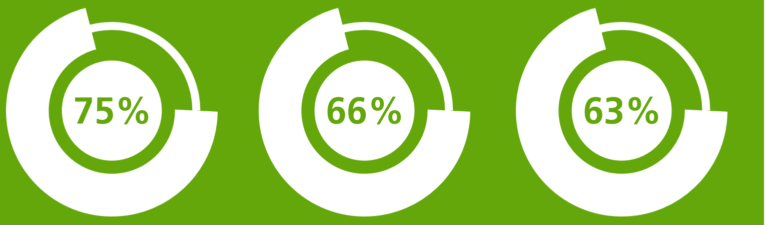
1. Understand your customers – for smaller merchants in particular, knowing your customers' buying habits and patterns will help identify any unusual behaviour.

2. Be vigilant – be suspicious of unusual behaviour as it could be a fraudulent transaction made using a stolen card. If in doubt, contact the customer to confirm the order. It might set alarm bells ringing and enable the merchants to halt the transaction if they feel it could be fraudulent.

3. Work with a PSP – Merchants don't need to go it alone. Whereas some of the bigger merchants might have their own risk models and the financial and reputational repercussions of a fraudulent transaction or data breach can be minimised and easily managed, for smaller players it could have devastating, long-lasting consequences. Working with an expert to help understand the options available could help put in place other payment methods which will minimise risk to merchants' businesses.

What you should now know

- The most common types of fraud causing concern among merchants are identity theft (71 per cent), phishing (66 per cent) and account theft (63 per cent).



- Fraud is not exclusive to credit card payments, with criminals becoming more sophisticated in their use of malware to command online banking logins via phones, tablets and computers, using the stolen bank account details to make fraudulent payments.
- “Friendly fraud” is particularly prevalent with services, including gambling and those in the adult milieus, where chargebacks are deliberately initiated, claiming credit card or account details were stolen.
- In “clean fraud”, criminals use sound analyses of the fraud detection systems deployed, plus a great deal of knowledge about the rightful owners of their stolen credit cards.
- To judge a payment type solely by its fraud risk is a mistake. If everyone did that, no merchant would ever accept credit card payments or SEPA direct debits.
- Credit cards are an integral part of online shopping, but a “healthy mix” is recommended. Online merchants should always offer “push” payment methods as well as including invoicing, prepayment and real-time bank transfer systems and schemes, all of which prevent misuse of sensitive data by not collecting it in the first place.
- To minimise the risk of fraudulent card transactions: understand your customers; be vigilant; and work with an expert to help understand the options available.

Read on to learn about the future of fraud

Section

3

Prevention and practical advice

PPRO

the payment professionals

Fraud prevention in e-commerce

Snapshot

- Two key fraud-fighting measures are appropriate risk management and know-your-customer (KYC) strategies
- Consider getting a partner, like a PSP, to take over your fraud management to allow you to focus on your core competencies
- As a rule, merchants should be more cautious when it comes to new customers
- PPRO's proprietary risk management system is called Evolve

It is important that administrator access to e-commerce systems is restricted to certain IP addresses or devices

Wherever business is done, fraudsters are never far away. There are, however, effective measures that can be taken to prevent e-commerce fraud. This section highlights measures for technical fraud prevention.

by Karsten Witke, Head of Payment Services Risk, PPRO Group

Two of the most important fraud-fighting measures are appropriate risk management and know-your-customer (KYC) strategies. Companies that know their customers well can minimise their risk of fraud. Detailed information on this topic can be found in the article on page 34. These measures should, however, be accompanied by additional technical fraud prevention methods. We've compiled a list of the ten most important points.

Point 1: Secure e-commerce platform

Choosing the right e-commerce platform can be tricky. When putting together your checklist for selecting an appropriate platform, don't just include performance and cost; instead, you should also consider security. It is, for example, important that administrator access to e-commerce systems can be restricted to certain IP addresses or devices. It is also important that anyone working on the system should identify themselves using complex passwords or – better still – two-factor authentication. Interfaces for risk management systems are a good thing. When it comes to fraud prevention, go all out.

Point 2: Multistep security

IT security is not achieved by a single measure or product. Instead a multistep process is the best approach. This involves enhancing basic security measures with additional ones. For example, firewalls should be used to protect e-commerce systems against attacks. Customers should interact with online shops only through SSL-encrypted sessions. Additional steps to securing your systems include checking all forms and entry fields for scripting vulnerabilities and hardening the databases used. You should also check your security measures regularly to ensure that they conform to the latest requirements.

Point 3: Meet security standards

Security is a wide field and there are a lot of products and services available. These, of course, cost money. "Do you really need all that?" is a legitimate question. And no, you don't. Security should be considered similarly to insurance. There's such a thing as "too much". Over-insuring things is not just expensive; it's impossible to keep it all in perspective.

Security standards, such as the Payment Card Industry Data Security Standard (PCI DSS), can provide guidance. This standard defines the security requirements for processing, storing and transmitting confidential card details. PCI DSS, for example, issues provisions for protecting networks which process credit card details. Protecting the data itself is also regulated. The standard also describes how access controls should look and what else should be taken into account when processing data – including current antivirus software, firewalls, and regular security checks, for example. When storing sensitive customer information, vendors should tread carefully (storing only the essentials) because the PCI DSS usually prohibits storing credit card numbers, expiry dates and CVV2 security codes. If this type of data must be stored, it can be done only with the prescribed type of encryption.

Point 4: Securing payment types

Payment types are not unassailable fortresses. For example, credit card data or PayPal login details can be stolen. There are, however, several additional measures that retailers can take to lock down this information. Take credit cards, for example: using address verification, requiring the CVV number, and using additional security functions like 3D Secure can protect against abuse and fraud.

Customers should also be informed that the same password should not be used for multiple purposes

Point 5: Strengthening passwords

"123abc","password" and similar passwords are absolute no-nos. Anyone creating a user account with an online shop must adhere to a few password rules. Fundamental security standards prescribe at least eight characters and a mixture of upper-case and lower-case letters, plus numbers and special characters. Customers should also be informed that the same password should not be used for multiple purposes. This does, however, not relieve retailers of their duty to safeguard user data on the backend. Two-factor authentication is better than simple password protection, as it requires customers to enter an access code in addition to their password. This code could, for example, be generated by a mobile phone app.

Point 6: Using alarm systems

Transactions in the shop should always be monitored and systems should be furnished with automated alarms. If someone makes purchases using several different credit cards within a short time frame, for example, or makes a lot of mistakes entering the address, or the address and telephone number provided do not match, the system should raise an alarm. More on the topic of fraud prevention through risk management and KYC can be found in the article on page 34.

Point 7: Tracking orders

One good method for preventing what is known as "friendly fraud" (see the article on page 18) is attaching tracking numbers to all orders. In friendly fraud, orders are placed and then chargebacks are deliberately initiated. This is a fairly easy thing to do with credit card payments or direct debits. Customers simply state that they did not place the order, or that they placed the order but did not receive the goods. Tracking numbers help you to keep an overview of all transactions and to ward off attempts to defraud more easily.

> Transactions in the shop should always be monitored and systems should be furnished with automated alarms

Point 8: Monitoring

Shopkeepers who want to know what's going on keep their eyes open, place mirrors in hard-to-see areas, and usually use video cameras. The online equivalent is a real-time monitoring tool which keeps an eye on customers' website behaviour and detects fraud more quickly. Servers on which commerce systems are running must be well locked down and monitored using a tool. These measures allow breaches to be detected earlier.

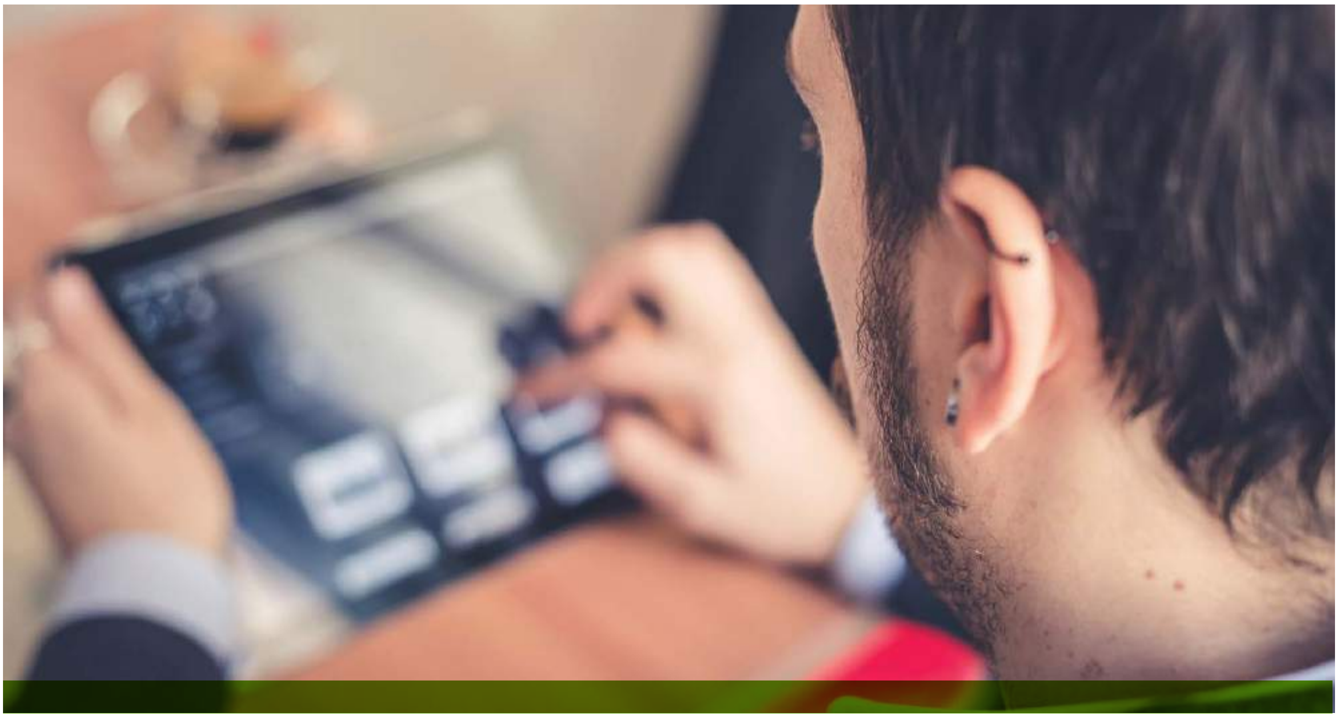
Point 9: Fraud management

Fraud attempts are always bad for retailers. They cost time and money, and cause stress. While smaller shops may be able to pursue fraudsters themselves, internationally active retailers will have difficulty doing so. This is where you should consider getting a partner, like a PSP, to take over your fraud management. Doing this allows retailers to focus on their core competencies.

Tip 10: Push, don't pull

Although no shop should refuse to accept credit cards as a payment method, retailers should set greater store by what are known as "push" payments, in which the purchaser, rather than the seller, initiates the payment. The big advantage is that there is no risk of chargebacks – and, in many cases, there is even a payment guarantee.

Know Your Customer (KYC) strategies protect against fraud



Merchants who know their customers well are best placed to use targeted methods to prevent fraud

Merchants who know their customers can minimise e-commerce fraud. The following real-life risk management and know your customer (KYC) strategies can help.

by Karsten Witke, Head of Payment Services Risk, PPRO Group

E-commerce fraud can be most effectively curbed by the use of two measures: technical protection (see article on page 38) and know your customer (KYC) strategies. After all, merchants who know their customers well are best placed to use targeted methods to prevent fraud.

Who are your customers?

The question at the heart of fraud prevention and risk management for merchants is: "Who are my customers?" Simply knowing your customer's name is obviously not the answer – but at least that's a first step. Names and addresses can be verified using simple checks, allowing merchants to quickly find out whether or not an address provided actually exists. Merchants can also do the same with payment information, like account details or credit card numbers. It is, of course, also important to collect email addresses or telephone numbers, as these can also be verified.

This information can best be collected via information services and integrated with online shops using plugins. This can provide targeted protection against several fraudster tricks, such as using stolen payment data in combination with fantasy addresses. Many payment service providers (PSPs) offer these information services as part of their portfolio. The advantage here is that PSPs also provide tools which monitor how orders, declinations and chargebacks develop according to the payment type and the fraud prevention method used.

The aim of these checks and this level of vigilance is to minimise bad debt losses and fraud by trying to determine early on (during the order process) whether a particular customer is "good" or "bad". While an order is being placed, the customer's name and location are being queried live with a scoring provider. The more data available, the better. During scoring, the data provided is run through a mathematical prediction process which determines a rating. This rating provides an up-to-date prognosis of the customer's future payment behaviour. Customers who receive a very good rating can be offered all payment methods, including invoicing, from their very first order. Customers with low scores, on the other hand, are shown only advance payment options. An additional advantage of the live test is that it can be used to identify stolen credit cards, as well as customers who initiate large numbers of chargebacks (reverse payments).

The aim of these checks and this level of vigilance is to minimise bad debt losses and fraud...

Limiting risks

The key to running an international e-commerce business successfully is to tailor your approach to customers in different countries and regions, based on cultural and payment preferences – no two countries have the same preferences. Merchants use a feature known as geotargeting to evaluate customer IP addresses. This gives them a fairly precise idea of where each customer is located. They can then make the appropriate language settings, as well as listing local payment preferences at checkout. The IP address is, however, also an important characteristic for risk management, as it allows orders from particular countries to be blocked.

Merchants use a feature known as geotargeting to evaluate customer IP addresses

Merchants should be more cautious when it comes to new customers

Another risk characteristic is targeted address concealment, which uses anonymising tools like proxies. In and of itself, address concealment is no reason to suspect a fraudulent order. However, if the IP address indicates one country, the customer selects a different one for the delivery address, and a throwaway email address is provided, risk management systems should warn the merchant (how risk management works in practice is explained by the article on page 38). Every transaction is checked by a set of rules and categorised as either “good”, “suspicious“ or “fraudulent”.

... a customer with an order history provides a great deal of comparison data for risk management

Classifying customers

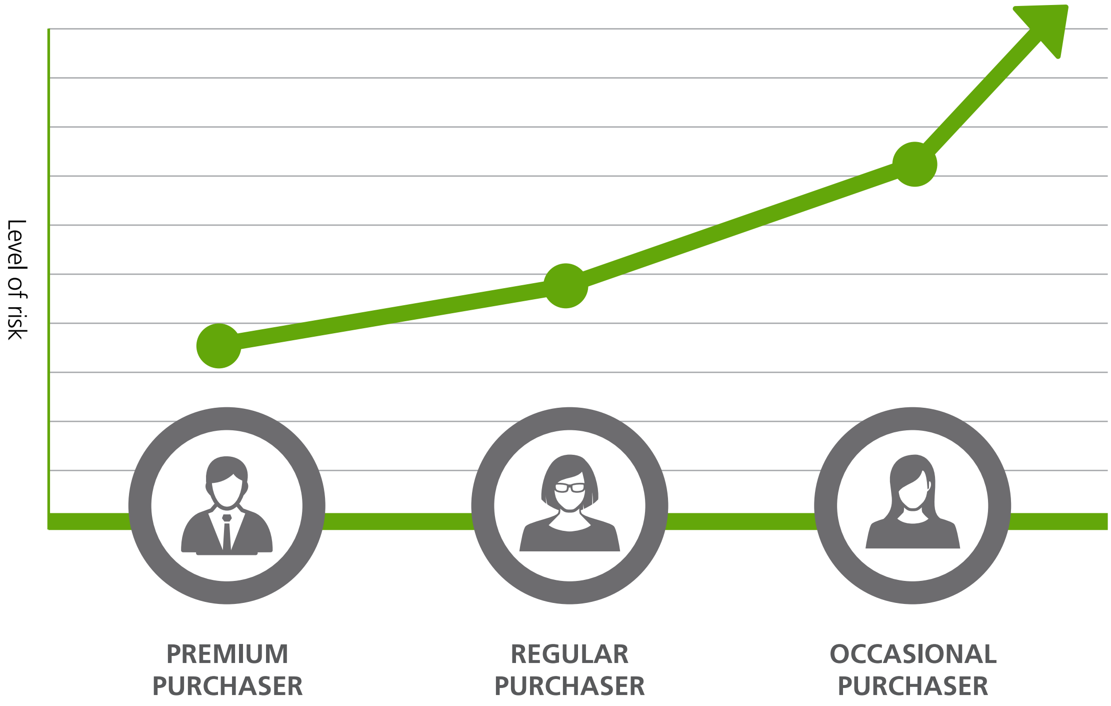
The aim of risk management is, of course, to minimise fraud, and customer accounts simplify the KYC process. After all, a customer with an order history provides a great deal of comparison data for risk management. If, for example, a customer spends an average of 50 euros once per month, a risk management alarm should be triggered when he or she suddenly places two orders totalling over 500 euros in a single day.

As a rule, merchants should be more cautious when it comes to new customers, and remain on the safe side by presenting customers with only low-risk payment options with their first orders, such as prepayment or other push payment methods, like giropay. In such cases, the customer actively sends the money to the merchant and the goods are sent out once the payment is received. One pleasant side effect is that push payments prevent merchants from having to figure out secure storage for payment information.

Merchants should, on the other hand, cater to premium customers by offering them a large selection of payment types. Here, typical favourite payment types, like invoice or direct debit for German customers, iDEAL for Dutch customers, and Alipay for Chinese customers, should appear right at the top of the list. It is not just that these customers always pay on time, but that they also trust your web store – and they bring in a certain amount of revenue. Depending on the size of the online shop, regular customers should, therefore, be divided into multiple categories, such as occasional purchasers, regular purchasers, and premium customers. Many popular shop systems allow merchants to define customer profiles based on customer payment behaviour and sales. Regular customers, of course, are offered more risky payment types like credit cards and purchasing on account, and those in European countries are given the option of using SEPA direct debit processes.

Knowing your customer well is not only an advantage for risk management. Clever merchants can also use their knowledge of their customers to create targeted marketing campaigns or special offers.

Do you know your customer?



Risk Management in Practice

Using risk management techniques to minimise the risk of non-payment is often described too academically. We take a look at the practical aspects and explain how PPRO's risk management system, Evolve, works in the real world.

by Sergej Pfeifer, Product Manager, and Andreas Sommer, Developer, PPRO Group

PPRO's "Evolve" determines whether a transaction is a fraud attempt or involves any other increased risks

PPRO use their proprietary risk management system, Evolve, for a variety of payment types. When it comes to risk management systems, distinctions are made between different theoretical approaches, with Evolve being what is known as a risk identification system. This means that Evolve determines whether a transaction is a fraud attempt or involves any other increased risks. To do this, the transaction data entered is analysed by a ruleset in order to determine a risk score. This enables transactions to be flagged as normal, suspicious, or fraudulent.

Flexible rules

One of the main advantages of the Evolve system, which was developed over several years, is that flexible rulesets can be used. Evolve allows different validation rules to be used for each payment type monitored. PPRO, for example, defined separate rulesets for monitoring credit card transactions and their own direct transfer payment option, InstantTransfer. More than 30 rules per payment type are unnecessary, as they don't just have to be executed one at a time: instead, they can also be combined. Risk managers can adjust each rule separately in the live system; this is important because risk management is an infinite process. A simple user interface is used to set up and test new rules, or to adjust existing ones.

Rules and threshold values

There are two threshold values per ruleset. If a transaction exceeds the first threshold value, it's classed as "suspicious"; if it then also exceeds the second threshold value, it's categorised as "fraudulent". Executing the validation rules results in a score, which is compared with these threshold values. A ruleset can be further restricted using filters, if specific rules (such as those for transactions from particular countries or selected banking groups) are to be executed.

If, for example, a user carries out an average of one transaction per month and suddenly makes a second and third purchase in a single day, an initial validation rule will raise an alarm. In and of itself, there is no reason to block the transaction – perhaps the customer is simply shopping for birthday gifts. Evolve determines a score, however, which flags the transaction initially as "suspicious". If the unusual number of transactions is then discovered to have been initiated from abroad, or the transaction amounts are unusually high, the threshold value for fraud is exceeded and the transaction is blocked. Key validation criteria are the customer number (ID) stored in the system, the transaction amount, the country where the transaction is initiated, the current IP address, and any negative history which could help to categorise the risk more precisely.

All or nothing

Scoring (the statistical estimation of fraud) is complicated and can result in complex rulesets because various rules – considered separately from one another – must apply and exceed the threshold value in order to block a transaction.

Evolve's rules have been developed over several years and constantly adjusted. Even so, the developers also decided to add an all-or-nothing decision-making function. Regardless of the score determined, therefore, a single broken rule can lead to a transaction being categorised as fraudulent and blocked. If a customer has initiated chargebacks for their last three credit card purchases, for example, their next transaction can be blocked without checking any other rules. Suspicious transactions can be sent through a series of additional checks.

Although using security procedures like 3D Secure for credit card purchases admittedly reduces the customer conversion rate, Evolve can be set up to ensure that 3D Secure is not required for normal transactions, yet remains obligatory for suspicious ones. Furthermore, the rules for known customers with positive purchase histories are less restrictive than those for new customers, for example.

If customers ask why a transaction was blocked, support staff need access to the risk management data

Support

Evolve stores the calculated scores in a database. There are two reasons for this: firstly, the decisions made are subsequently re-evaluated, and secondly, the information is important for customer support purposes. If customers ask why a transaction was blocked, support staff need access to the risk management data. Sensitive data like bank account details, on the other hand, remains in Evolve only for verification purposes and is not stored permanently.

Automation and blacklisting

Blacklisting and whitelisting, as well as aspects of automation, are currently being expanded. During blacklisting and whitelisting, the KYC (Know Your Customer) data is used even more intensively: it can be used to add customers with negative histories manually to a blacklist, whereas good customers can be whitelisted and are allowed considerably more leeway. New automated features are designed to make more efficient use of additional information sources. These include chargeback information from the credit card companies, country block lists, and automatic recognition of stolen credit card data.

What you should now know

- To know your customer make sure you have their name, address, credit card numbers, email address and/or telephone number and then verify them.
- When storing sensitive customer information, vendors should tread carefully as the PCI DSS usually prohibits storing credit card numbers, expiry dates and CVV2 security codes.
- Real-time monitoring tools can keep an eye on customers' website behaviour and detect fraud more quickly.
- A potential customer's IP address is an important characteristic for risk management, as it allows orders from particular countries to be blocked.
- Evolve allows different validation rules to be used for each payment type monitored.
- Knowing your customer well is not only an advantage for risk management. Clever merchants can also use their knowledge of their customers to create targeted marketing campaigns or special offers.
- Evolve can be set up to ensure that security procedures like 3D Secure is not required for normal transactions, yet remains obligatory for suspicious ones.

Read on to learn about the future of fraud

Section

4

The future of fraud

PPRO
the payment professionals

Innovation versus risk: have we got it wrong?

There have been countless articles over the years bemoaning how risk and regulation hinders innovation. However, there are always two sides to a coin so is this media coverage fair? Is there an argument that risk and regulation can actually be a driver to innovation?

John Fernandez, Legal Counsel, PPRO Group

A recent poll we carried out highlighted the significant impact of innovation: according to just under a third of UK merchants (31 per cent), e-wallets were the most popular payment method, suggesting that they now hold a position of trust for today's online shoppers[1]. Retailers understand that payment demands are changing, with over three quarters (77 per cent) of those we surveyed interested in keeping up to date with the range of online payment methods available.

There are some merchants that are risk averse, in particular when presented with the opportunity of international markets, but they could be missing out on valuable international revenue by resisting change. Despite on average one in every five transactions (19 per cent) being made by international customers, nine out of ten (90 per cent) retailers remain more interested in attracting domestic customers than those from overseas. Merchants could be missing out on an important audience, with nearly one in ten (8 per cent) admitting that between 31 and 51 per cent of all transactions come from international customers.

Snapshot

- **Innovation in e-payments has a huge impact upon how merchants view and manage risk**
- **Generational differences plays a part in the consumer adoption of emerging payment methods**
- **Rather then stifling creativity and risk, new regulations can actually increase innovation in payments**
- **PSPs must master more than mere technology but know the answers to regulation-related questions**

Notes

1 "Crossing Borders – The Evolution of Online Payment Methods and Impact Upon International Trade" – Coleman Parkes for PPRO Group, November 2014
www.wzb.eu/en/press-release/people-in-poorer-countries-show-higher-tolerance-for-risk

No two retailers are alike

Every business will have a slightly different risk profile that will be driven by how risk averse those steering the business inherently are. Having said that, a risk profile can change over time, with older established businesses – especially those in heavily regulated industries or those susceptible to fraud – generally being more risk averse as they have had their fingers burnt before.

Innovation is often born out of necessity. For traditional, risk averse merchants this is because they are having to compete against a rising number of new entrants from increasingly diverse channels that have progressive business models designed around the wants and needs of a 21st century consumer. At the back of their minds, none of them want to be the next Borders or HMV.

Risky payments

It is interesting when some think that modern payment mechanisms such as the likes of Apple Pay are risky. They are actually a good example of innovation that started with the widespread adoption of PayPal. These emerging payment mechanisms all have one thing in common, they circumvent the use of traditional credit cards, which themselves are an inherently risky payment mechanism to use online simply because they weren't originally meant to be used in that way. Credit cards are particularly open to fraud as they were designed for use in the physical world where the common authentication mechanisms (ID, signature, PIN etc.) simply don't translate to being used by merchants in the online realm.

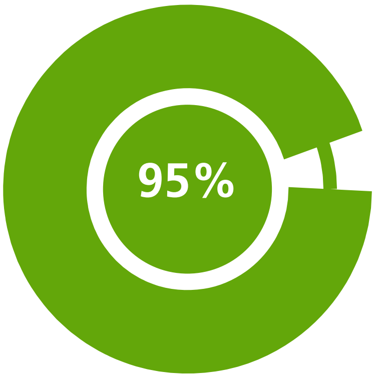
To compete, the humble credit card has had to evolve in its attempts to be more secure and cut down on fraud: two factor authentication (2FA), biometrics and making the card details 'hashed' and invisible to the merchant are famous examples of this.

Yet, it's not just those payment methods born in the traditional world, but emerging payment methods can also be open to the scourge of fraud, so retailers and consumers both need to be mindful of them. Nearly all of those businesses we surveyed (95 per cent) admitted that fraud is still a concern when it comes to online transactions. It is clear that despite a willingness to adopt additional payment methods, businesses are still wary of the wider associated risks of doing so.

Who are the risk averse and the risk takers?

One of the main catalysts for risk is whether the consumers you are wishing to target are risk takers themselves. One prime example is if you are targeting the younger generation, who throughout the annals of time have always been risk takers, in fact it is the same now as it was when I was one myself.

As well as generational difference, there is also a difference in consumer risk appetite on a geographical basis. Historic thinking was that consumers from emerging markets are more risk averse, as intrinsically they have



Nearly all of those businesses we surveyed admitted that fraud is still a concern when it comes to online transactions

Notes

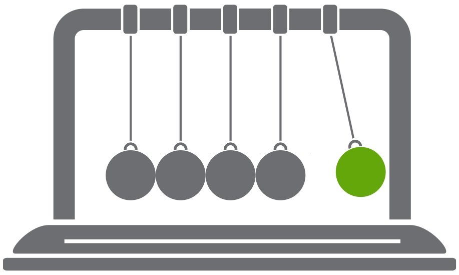
[2] www.wzb.eu/en/press-release/people-in-poorer-countries-show-higher-tolerance-for-risk

very little so want to protect it. Whereas consumers in developed markets governed by established law and order, and with consumer protections in place have the right environment to take more risks.

However, new research[2] from WZB Berlin Social Science Centre, which looked into the risk-taking preferences of over 3,000 people across 30 countries appears to contradict previous theories, reaching the conclusion that the higher the per capita income, the lower the willingness to take risks. In fact, people in Ethiopia, Nicaragua and Vietnam were the most enthusiastic risk-takers in the study. Times are changing and new e-commerce markets are rapidly taking shape in unanticipated ways and regions. The merchants who keep their fingers on the pulse of these changes and opportunities will inevitably stay one step ahead of the competition.

An unexpected catalyst

Something interesting generally happens when new regulations are imposed. Rather than stifling creativity and risk, what we actually see is that innovation increases as businesses need to tune their operations to adhere to the new regulations. Rather than being painted with the brush of being the stuffy older statesmen of the industry, the regulators could be thought of as the true innovators!



...the pendulum is swinging towards the risk takers, so more conservative businesses need to sit up and take notice

The risk pendulum is constantly swinging back and forth. As the world is, on the whole, coming out of the recession of the last few years, the pendulum is swinging towards the risk takers, so more conservative businesses need to sit up and take notice. However, inevitably it will swing back again when risks are taken to the extreme.

With online shopping now the norm among consumers and businesses, online merchants have had to step up their game in recent years when it comes to converting browsers into buyers. With shoppers now much more open to buying from overseas websites, retailers have needed to adapt and embrace new options familiar to those outside of the UK in order to appeal to a much broader reach and global clientele. All the while treading the fine line between innovation and risk.

Regulating Tomorrow

The directive aims to make cross-border payments as simple, efficient and secure as those carried out within member states

Simply being up to date is no longer enough. PSPs must be equipped for the future and at least one step ahead in their services. The good news is that keeping up with regulation is not overly difficult, provided that you take into account a few key points.

John Fernandez, Legal Counsel, PPRO Group

PSD2 and MIF might sound like innocuous acronyms, but they have the potential to significantly impact and alter the payment landscape in the long term. Indeed, the second Payment Services Directive (PSD2) and Multilateral Interchange Fee (MIF) regulations are currently the subject of a great deal of discussion. PSD2 has a broad scope and forms the legal basis for the creation of an internal EU payments market. The directive includes provisions which apply to all payment services in the European Union, and aims to make cross-border payments as simple, efficient and secure as those carried out within member states. It is also designed to improve competition by opening up payment markets to new providers.

The MIF, on the other hand, is all about regulating the level of interchange that are paid by the merchant's acquirer to the card issuer to compensate for enabling, authorising and clearing a card transaction. Following a number of heated debates, the future of the legislation has been decided.

Some of the key provisions include prohibiting cross border transaction fees from exceeding 0.2% (for debit cards) and 0.3% (for credit cards). It is proposed these caps apply to domestic transactions 2 years after MIF is implemented. With the changes coming into force towards the end of 2015, it will take months to analyse the exact cost position and merchants might not see any immediate savings at all. Additionally, acquiring banks will no longer be permitted to charge merchants a blended fee – they must charge individually for different categories and brands of payment cards unless merchants request so otherwise in writing. It will be permitted for payment cards themselves to be co-badged (i.e. the branding of different card payment schemes on one card) and consumers will be allowed to choose which brand they want to use at the point of sale. Finally the "honour all cards" rule will be limited and retailers will no longer be prevented from steering consumers towards the use of specific payment instruments.

A regulated PSP must know these rules by heart if they are active in Europe. However, as every country has its own financial regulatory authority[1], the EU regulations for international PSPs are not the only ones which must be taken into account. The following insight and advice will use PSD2 as an example, giving key starting points to help PSPs stay one step ahead when it comes to regulations.

> ...the PSD states that, as of 1 January 2012, transactions to a payment account must be credited to the account at the latest by close of business one banking day after the payment order is placed

Regulation is slow-moving

The payment industry is dynamic, with major players from various industries and small innovative companies launching new payment products and services every week. As many new inventions in the payment field are driven by technology, the payment market is currently filled with the hustle and bustle of the IT industry – and what is news today is forgotten tomorrow. PSPs, however, must master more than mere technology. Instead, they must also know the answers to regulation-related questions – a topic which is anything but dynamic. As the PSD illustrates, regulations can be slow to develop and adopt.

The original Payment Services Directive from 2007 is still the basis for domestic law in EU member states[2]. The PSD governs such matters as the information requirements for payment services: What information must a provider share with their customers, and when? How quickly must payments be carried out, and which reimbursement requirements are there? In order to speed up payments, the PSD states that, as of 1 January 2012, transactions to a payment account must be credited to the account at the latest by close of business one banking day after the payment order is placed. The PSD was adopted in 2007, so this particular change was afforded more than four years to implement.

The PSD's successor: PSD2

In addition to prescribed time frames, directives themselves cannot be adapted or adopted overnight. Instead, they are created via a long political process involving a great deal of lobbying from various industries. Discussions on the PSD's successor – PSD2 – have recently been finalised. In May 2015, the first political agreement was reached in negotiations between the Commission, The European Parliament, and the Council of

Notes

[1] www.en.wikipedia.org/wiki/List_of_financial_regulatory_authorities_by_country

[2] www.eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32007L0064

the European Union. Proposals for PSD2 were, however, first presented by the EU Commission in July 2013, almost two years beforehand.

PSD2 defines several priorities, one of which is to strengthen the security requirements for online payments. Specifically, customer authentication should be strengthened in order to mitigate fraud. In addition, PSD2 is intended to provide a legal framework which will further stimulate competition, thus benefiting market launches by new providers and the development of innovative mobile and internet payment methods. It also has a significant technical basis to it: the European Banking Authority (EBA) is to develop guidelines and drafts of technical regulatory standards for various industries.

PSD2 however, even after officially being adopted, will still require another 18 months prior to being implemented domestically and its provisions becoming applicable under national laws.

Getting a grip on today's regulations

How should PSPs prepare themselves for regulatory issues? Keeping up with legislative instruments such as the PSD or guidance documents issued by regulatory authorities is key. Within the EU, most regulatory authorities adopt a transparent approach and provide such information via official websites. If this seems like too much effort, a great many practical guides are available online, such as PSD implementation instructions[3]. Not every PSP can keep tabs on political minutiae, so good summaries of current developments are available[4]. When it comes to international regulations, the local financial regulatory authorities are generally the first point of contact.

Keeping up with legislative instruments such as the PSD or guidance documents issued by regulatory authorities is key

Notes

[3] www.europeanpaymentscouncil.eu/documents/Brochure-%20 24-08-09-PSD-Web.pdf

[4] www.ecommerce-europe.eu/position-papers

This is clearly a complex topic in which expert knowledge is required and regarding foreign documents, there's the additional issue of the language barrier. This is where expert networks come into their own. PSPs can make contacts in international expert networks either directly or via organisations such as the Electronic Money Association (EMA)[5].

Fit for the regulations of the future

For those who want to know about the future of regulations as early as possible, industry bodies such as the EMA are an indispensable resource and also dispatch members to other expert groups who then, in turn, advise the European Commission. The Payment Systems Market Expert Group (PSMEG), for example, draws up legal proposals on financial services for the Commission. There are, of course, also major panel discussions concerning regulatory topics in the payment industry at specialist conferences such as Money 2020 (which will, from 2016, also take place in Europe in addition to the main conference in the USA), or the annual PayComm MEETS Europe conference[6], where current and future trends are discussed. PSPs which take part in such events should, therefore, always be up to the minute, which allows them to future-proof their services early on.

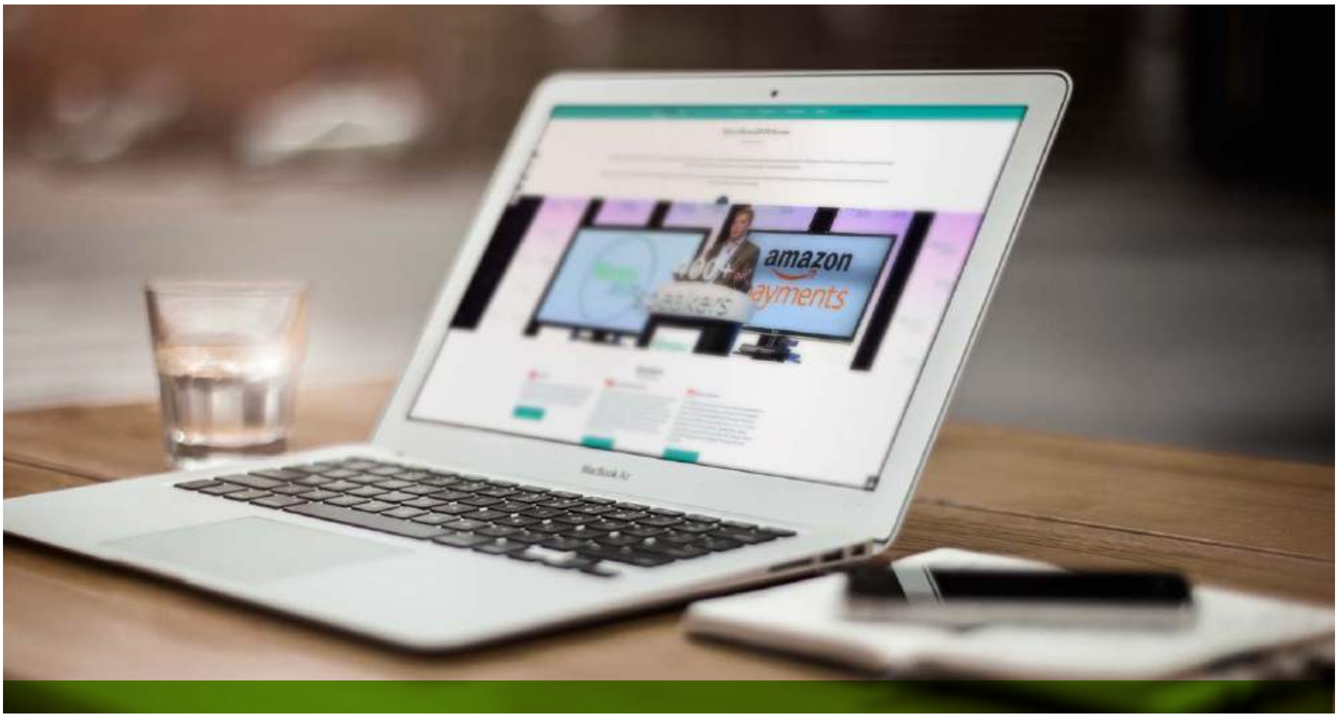
The regulatory mills grind slowly and those PSPs who approach the topic seriously will never be surprised by what happens next. Remaining up to date on the development of regulation will ensure the right policies and procedures are put in place for organisations in good time. Keeping in contact with financial regulatory authorities across the globe will equip PSPs with invaluable information on special regulations. Supplemented with insight from conferences and expert panels from organisations such as the EMA, PSPs can not only best equip companies for the future, but can help to shape it.

PSPs can make contacts in international expert networks either directly or via organisations such as the Electronic Money Association (EMA)

Notes

[5] www.e-ma.org

[6] www.money2020europe.com/; www.paycomm.de/en/pub/public_area/paycomm_conference.php



IMPORTANT INFORMATION RESOURCES FOR REGULATORY ISSUES

Financial Regulatory Authorities

- Country overview

Associations (Examples)

- EMA – Electronic Money Association
- GEMA (Gibraltar E-Money Association)
- CEESCA (Russian Electronic Money Association)
- ECA (European Compliance Academy)

Conferences (Examples)

- Money 2020
- Money 2020 Europe
- PayComm

Standards and Practical Guides (Examples)

- PSD
- PSD Implementation
- PCI (Payment Card Industry)
- E-commerce Europe (ecommerce-europe.eu/position-papers)

News Sources (Examples)

- Risk and Compliance magazine
- Compliance Week
- Compliance Insider

What you should now know

- Merchants who are risk averse could be missing out on valuable international revenue by resisting change.
- Emerging payment methods circumvent the use of traditional credit cards, which are an inherently risky payment mechanism.
- With shoppers much more open to buying from overseas websites, merchants need to adapt and new options familiar to those outside of the UK.
- A regulated PSP must be aware of all EU payment regulations if they are active in Europe, as well as country specific regulations if they are to operate successfully on a global scale.
- To remain prepared, PSPs need to keep up with legislative guidance documents issued by regulatory authorities.
- As many new inventions in the payment field are driven by technology, the payment market is currently filled with the hustle and bustle of the IT industry - and what is news today is forgotten tomorrow.
- The Payment Systems Market Expert Group (PSMEG) and specialist conferences such as Money 2020 or PayComm MEETS Europe conference are also indispensable resources for insight and guidance about the future of regulations.

Read on to learn about the future of fraud

Payment schemes and risks

Category	Form of usage	Devices	Associated risks (for merchants/PSPs)	Any solutions?
credit cards	contactless/ online/ offline	POS/mobile	- chargeback - friendly fraud - data theft	- know your consumer - scoring risk systems - velocity checks
debit cards	contactless/ online/ offline	POS/mobile	- chargeback - friendly fraud - data theft	- know your consumer - scoring risk systems - velocity checks
prepaid cards	contactless/ online/ offline	POS/mobile	- chargeback - friendly fraud - data theft	- know your consumer - scoring risk systems - velocity checks
local card schemes	contactless/ online/ offline	POS/mobile	- chargeback - friendly fraud - data theft	- know your consumer - scoring risk systems - velocity checks
e-wallets	online	mobile	- fraud requests from scheme or authoritie - friendly fraud - data theft	- know your consumer - scoring risk systems - velocity checks
real-time bank transfer	online/ offline	mobile	- fraud requests from banks or authorities - friendly fraud - data theft - "missing funds"	- know your consumer - allow mobile TANs only - scoring risk systems - velocity checks - use guranteed schemes - monitor and be aware of "missing funds"
direct debit	online/ offline	mobile	- chargeback - friendly fraud - data theft	- know your consumer - mandate from consumer - scoring risk systems - velocity checks - monitor chargebacks - do not offer to new consumers (only bank transfer first)
electronic cash payments	online	POS	- takes long time to complete; high risk of consumers not finishing a transaction - data theft	- know your consumer - scoring risk systems - velocity checks
crypto currency	online	mobile	- money laundry risk - FX risk - data theft - "bad name"	- know your consumer - scoring risk systems - velocity checks
pay-out	online/ offline	POS/mobile	- data theft	- know your consumer

Author biographies

Simon Black, *CEO, PPRO Group*

Simon Black, MBA in Business from Georgetown University has extensive experience in consulting and business, and in his early career founded a marketing software start-up company as well as holding senior strategy and brand consulting roles both in the USA where he lived for six years, and in the UK. Simon joined The PPRO Group as CEO in March 2015 following a decade with Sage Pay, 8 years of which he held the CEO position. Simon led the company through dramatic growth to become the UK's leading payment gateway for SMEs. He also led the creation of Sage One, the leading online accounting and payroll application. Simon has provided expert commentary on live TV and radio, has been published widely in payments and eCommerce media and has spoken at events such as Internet World and eCommerce Expo.

Andrew Edem, *Head of Engineering & Information Security Officer, PPRO Group*

Andrew has over 15 years of experience in software engineering, project management and information security in the financial and telecommunications sectors. Before joining PPRO in 2010, he co-ordinated software and infrastructure projects for issuing Visa and MasterCard Prepaid cards at Transact Network Limited.

At PPRO, Andrew is responsible for leading the engineering department responsible for design, implementation and operation of PPRO's payment processing and card issuing platforms, as well as for information security within the organisation as a whole.

John Fernandez, Legal Counsel*, PPRO Group*

John is a legal professional with a Bachelor of Laws (LLB) from the Victoria University of Wellington. He has comprehensive experience in compliance across e-commerce, new payment technologies and online payments for an international financial institution. His practice areas are financial regulatory law, cross border, e-commerce, e-Money, AML and financial services.

John has worked for the PPRO Group since 2010 as a Legal Counsel. In this role, John is responsible for advising on retail client business matters and market regulatory developments, as well as advising on corporate matters, board/shareholder processes and intercompany arrangements. John also monitors adherence to internal compliance procedures and processes (KYC, AML, FATCA) and oversees all EEA financial licensing applications.

Ralf Ohlhausen, *Chief Strategy Officer, PPRO Group*

Ralf Ohlhausen, MSc in mathematics and Master of Telecommunications Business, has over 25 years' experience in e commerce, financial services, mobile telecommunications and IT. Before joining PPRO Group, he was President Europe at SafetyPay. Other management positions on his international career path took him to Digicel, O2, British Telecom and Mannesmann-Kienzle. At PPRO, Ralf is responsible for increasing PPRO's global reach, focusing in particular on the addition of new payment choices to the company's portfolio.

Sergej Pfeifer, *Product Manager, PPRO Group*

Sergej has been a product manager and product owner at PPRO since January 2015. Previously, he was an international product manager at Sofort, provider of Sofort Banking. As the product owner for PPRO's alternative payment methods in payment processing, Sergej focuses on growing the company's APM-portfolio from a product management perspective. In addition to external payment methods, he is responsible for InstantTransfer, PPRO's own solution for real-time bank transfers. Sergej also takes care of WKV.com, an official online reseller of paysafecards, another significant PPRO business unit.

Andreas Sommer, *Developer, PPRO Group*

Andreas has an M.Sc. in Informatics and joined PPRO as a software developer in January 2015. His responsibilities, amongst others, cover the payment scheme InstantTransfer, the risk management service Evolve, the internal test environment and tooling.

Rick Terra, *Managing Director, Intrum Justitia (Netherlands)*

Rick Terra was born in Friesland in the northern part of Holland. He studied in Groningen at the Hanzehogeschool and holds an MSc in management and organisation at Tias Business School. From 2000 he worked at KPN in Groningen and The Hague and held the position of Manager Collection Management from 2005 until 2008. In 2009 he won the Credit Manager of the Year Award. Rick joined Vesting Finance as Director of Operations and later as Director of the Business Unit Collection services.

In March 2015 he joined Intrum Justitia as Managing Director. Intrum Justitia is Europe's leading Credit Management Services (CMS) group, offering comprehensive services, including purchase of receivables, designed to measurably improve clients' cash flows and long-term profitability. Founded in 1923, Intrum Justitia has some 3,800 employees in 20 markets. Consolidated revenues amounted to SEK 5.2 billion in 2014. Intrum Justitia AB has been listed on Nasdaq Stockholm since 2002.

Karsten Witke, *Head of Payment Services Risk, PPRO Group*

Karsten Witke has many years of risk management experience in the financial industry. Before joining the PPRO Group in 2011, Karsten worked for six years in Risk and Operations at Wirecard Payment Solutions and INATEC Payment AG. In his position at PPRO, Karsten Witke leads the Risk and Boarding Team and as Head of Payment Services Risk is responsible for all processes related to risk management and fraud prevention. This includes the onboarding of new customers and the accompanying KYC processes, as well as the analysis of potential risks and cases of fraud. He works in close collaboration with customers and PSPs and is one of the key contacts for corporate clients. As a specialist in alternative payment options, Karsten provides advanced training in this area to customers and partners worldwide.

PPRO Financial Ltd
23 Hanover Square, London
W1S 1JB, United Kingdom

T: +44 (0)203 0029 170
E: marketing@ppro.com

www.ppro.com

PPRO
the payment professionals