Fraud Trends 2016

Latest perspectives on international eCommerce fraud

June 2016
Introduction

eCommerce is growing. In fact, we have predicted (see our 2015 Global payments Report), that the global eCommerce market will be worth a staggering US$ 2.4 trillion by 2019. This brings an accompanying rise in fraud.

In short, online payment fraud is a bigger challenge than ever.

Meeting this challenge is not easy and how best to address the challenges affecting online merchants is a subject of much debate. This Worldpay research report focuses on certain key issues that are at the fore of discussions in the global risk/fraud market. Some, such as perceptions of mobile fraud, are acknowledged trends that merit a pulse-check. Others such as the effective use of a business’s data assets and the use of social media in fraud prevention are areas where Worldpay wishes to drive forward the debate.

This research combines research on four current topics as well as our own insights as a world-leader in payment solutions to explore the key challenges and opportunities facing global merchants now and in the future.

Methodology

This report has been compiled from a combination of qualitative and quantitative data, coupled with Worldpay’s own experience in payment technology and fraud.

Quantitative data

A detailed questionnaire was distributed in three ways:
- At Merchant Risk Council Event in Las Vegas 2016
- Posted to selected professional audiences on social media
- Emailed to a list of Worldpay customers

Results from some 200 respondents were collated and analysed for inclusion in this report.

Qualitative data

In-depth interviews were conducted with senior personnel from six major eCommerce merchants, all of which implement sophisticated strategies to minimise fraud.

Worldpay experience

As a leader in global payments, with over 400,000 customers worldwide, we have wide experience of addressing all types of payment fraud.
Executive summary

Today, there is widespread recognition among online merchants that fraud is a major issue. And, while merchants vary widely in their level of preparedness for handling this threat, there is also broad agreement on the ways it can be mitigated.

The majority of merchants, for example, believe that assessment of more data points will play a key role, and that there is scope to use data more effectively. Most merchants also see social media as an increasingly important tool in fraud prevention.

Key findings

- Transactions made with mobile devices are still treated the same as other transactions
- Social media is used in manual review, but is very time-consuming
- Data could be used more effectively by most organisations
Mobile: time will be the test

There are significant additional risks in the mobile channel, due to factors such as low use of 3DS, and vulnerability to malicious apps.

Despite this, most merchants assess mobile transactions in the same way as transactions from other platforms; they embrace mobile as just another channel and treat transaction fraud holistically.

Social media: nascent potential

While social media is not yet used to its full potential, its value is increasingly understood. Although merchants vary in the way they see it being used, all are interested in new ways to tap this rich source of insight, and over half of our respondents would like to make better use of it.

Many assess social profiles in manual review but this is very time-consuming, while some merchants collect social information but do little with it at present. Overall, it’s clear that the formal use of social media to fight fraud is still in its infancy.

Future of fraud: proactive fraud teams see risks ahead

The fraud landscape is shifting constantly as fraudsters try to evade ever-evolving detection techniques. Fraud professionals are highly informed about new threats and concerned about data breaches and new attack types.

However, as user expectations of a frictionless payment experience increase, businesses have to increasingly balance the differing needs of fraud teams and user experience. Merchants agree that increased automation and use of more data assets will be at the heart of progress. There is also likely to be ever greater use of social data as a way of establishing trust in a transaction.

Data is power

Merchants agree that they need all the data they can get to better assess transaction risk. However there is often data available within a business that is not fed into the fraud system, meaning that greater collaboration across teams would drive enhanced results.

Merchants also commented upon the value of external data sources when fighting fraud: those with the most sophisticated in-house tools still seek the insight provided by a data pooling approach. Meanwhile, there is a clear view among many merchants that machine learning and automation has much to offer, though manual reviews will remain important for high risk transactions.
High understanding of increased risk

59% of respondents state that they fully understand the increased risk relating to transactions made on a mobile device. It is likely that 3DS is avoided on a mobile device, so the transaction is unsecure. Also users rarely use anti-virus software on their mobile devices. Meanwhile, malicious apps can re-route information to fraudsters, and there is increased vulnerability from rooted or jailbroken devices.

The jury is still out

Despite the above, mobile is clearly a contentious topic. Although many (53%) merchants track the source of a transaction, and 59% believe that there is increased risk relating to mobile, a large proportion (67%) treat mobile transactions no differently from others. The overall position of respondents is reflected in a comment from one of our in-depth interviews: “We do track which channel transactions come from,” said the interviewee, “but [we find] the risk associated with mobile to be no different to anything else at this point.”

From one of our respondents

“Mobile is important, as it takes off we may see that things are different on the fraud/risk front. We’re not sure how we would deal with that.”
Some quotes from our respondents

“We do track which channel transactions come from but we find the risk is no different at this point.”

“We have not specifically looked at the difference between mobile fraud and what we see on a browser.”

“Mobile is where all the growth is, as everyone knows.”

Mobile payments will increase by 42% in 2016, reaching $617 billion.
Social media
Valuable insights but manual assessment

Today, the use of social media data in fraud prevention creates relatively little 'noise' in the industry. Despite this though, its value is increasingly understood, with almost 60% of respondents already using social media data in their review processes and 52% ready to make better use of it but lacking the knowledge of how to do so.

This could partly be because current usage is ad-hoc and manual. There is also a perception that the use of social media using manual techniques could be seen as opportunistic or subjective.

The search for reliable identity

For most respondents, the principal reason for using social media in a KYC or fraud prevention context is to check that an account and therefore an individual’s identity is real. To do this, manual reviewers make an assessment based on factors such as quantity of photos, conversations and posts.

However, the majority of respondents felt that, while valuable, these reviews are highly time-consuming and that they would welcome an automated way to derive the same insight. One participant commented, “We use social to verify that a purchaser exists, if they are who they say they are, is it a fake account...but it’s difficult if the name is John Smith. It (is) very manual.”

It was noted that reviews can provide proof-points in chargeback defence.

“We use social to verify that a purchaser exists, if they are who they say they are, is it a fake account...but it’s difficult if the name is John Smith. It (is) very manual.”
Social sign-on: a rich source of information

Social sign-on continues to gain traction as a way to help users avoid remembering numerous passwords, while offering the merchant valuable insights about their customer base. 35% of our participants currently offer social sign-on as part of their customer login processes.

Other Fraud and Payment professionals surveyed, however, were unsure whether this functionality was used within their business. There’s clearly a missed opportunity here for many businesses: social data could be used as a proactive part of fraud prevention, notably in the positive assessment of consistent identity information at registration and payment. Our research bore this out, with a high 56% of respondents stating they’d place greater trust in customers who use social logins.

It is of course essential that trust is placed only in valid profiles and, as such, that companies protect themselves with robust, automated means to determine profile validity.

Risk decisions are trust decisions

Among respondents, there was a generally high ‘neutral’ response rate on many issues, indicating that the formal use of social media to fight fraud is still in its early stages of growth. But the fact that 56% of respondents placed greater trust in customers who corroborated their identity at sign up, using a social media site, underscores the fact that risk decisions are essentially trust-based decisions.

The acquisition of consistent identity information about a customer is an important way of increasing trust.

The conclusion must be that, while social data usage is still largely informal, it’s extremely useful and business should consider tapping this rich vein - ideally with more formalised, consistent and time-efficient processes.
Data overload
Knowledge is power

Fraud teams are always keen on more data to drive better decisions. 77% of participants feel this particularly strongly for non-card payment methods where, typically, a minimal data set is provided with a transaction.

Attributes such as Device ID are obviously key tools in these scenarios, both because they are rich sources of insight but also because they are collected invisibly without requesting data capture from a purchaser and therefore do not impede a frictionless customer experience.

“The more data sharing we have, the less friction for the customer and the better (their) experience.”

“We could be using data a lot more effectively. I think we are not there yet.”

“There’s always data available that we don’t use.”
More insight could be leveraged

Although many businesses collect data to enable real-time risk assessment, most feel that there’s always more data that could be used to fight fraud. Only one company felt that it has all the data it needs.

It is of course necessary to distinguish between internal data sources such as customer purchase history or typical spend and external data sources such as device and behavioural information.

The former is often available already within a business and can be used to inform a richer risk decision at little cost to a business, if a company can communicate across functions. 58% of respondents said they know there’s lots of useful customer information within their business that they do not currently use to fight fraud, and respondents felt strongly that they could do more by feeding their risk engines with more internal data. “There is a lot more that could be used to detect a bad purchase,” said one respondent. “[Often] the information is all there, and I could have told you it would result in a chargeback, but we did not have the data points.”

Meanwhile, sharing of positive data is as important as sharing negative data. Social log-in data is one example where a Marketing team may collect valuable positive customer information at sign-in, but this may not be transmitted to a Fraud team’s decision engine.

There is a potential correlation between the age of a company and its use of data, with younger companies having established their process to be data-driven from the outset, with integrated systems and using the latest techniques and providers. Many large or established businesses need to deal with disparate systems obtained through regional expansion or company acquisition, making it very difficult to gain a single-customer view in order to implement more data-driven decisioning.

“We could be using data a lot more effectively; we’re not there yet.”
Machine learning continues to drive results

In our qualitative research, merchants shared their thoughts on machine learning. Most businesses agree that automating data analysis can uncover subtle and unexpected trends that can indicate fraudulent behaviour. Although most businesses are aware that correlation does not necessarily indicate causation, the deep trends and connections revealed by this kind of analysis can be a powerful predictor of fraudulent intent. “We get things popping up in big data that no one would have thought to ask,” said one interviewee, and when we look at these things, we can find disguised behaviour.”

Machine learning is, as one of our interviewees put it, an established way of determining “where the answers are.” The approach allows merchants to collect very large amounts of data and derive insights which they find to be relevant and actionable.

Machine learning can be used to develop strategies for:
1. Enablement (approving purchases that are declined by overly blunt rules)
2. Risk avoidance (declining or shifting liability of high risk transactions)
3. Efficient resource allocation (deciding what are the top priority purchases for manual review)

The value of sharing

There is wide agreement that, no matter how strong an organisation’s internal data, there is immense value in sharing data. Finding methods with which merchants can easily share data will help in the identification of fraud. Indeed, the vast majority of merchants using in-house fraud tools feed their systems with external data inputs for a broader view of fraudulent behaviour.

The death of manual review?

Does increased automation mean that the fraud team is on its way out? Not according to our research. Another important point that emerged was the importance of manual reviews for high risk transactions. While some businesses rely fully on automated analysis, most emphasise the value of human interpretive and analytical skills in some situations. Many pointed out that machine learning still needs human input to be useful. Effective fraud prevention strategies use machine learning both to automatically approve/decline clearly good/bad transactions, as well as to ensure human resources are focussed on high priority cases that do require a manual review.
An arms race

Fraud and Payment experts are very future-focused, with 93% saying they’re constantly planning ahead and are very interested in new technologies. They have to be: as businesses develop ever-better fraud detection techniques, fraudsters themselves become ever smarter at bypassing these techniques.

One particular theme that emerged in our interviews is that fraudsters are getting increasingly good at emulating legitimate behaviour, making it harder to detect fraudulent patterns – probably one of the reasons why only 63% of respondents felt completely in control of what fraud might hit their organisation in future.

As a result, most businesses are interested in any new technology that can keep them a step ahead of criminal activity. It becomes more critical than ever to use a portfolio of techniques. For example, Device ID, while a highly robust detection method, is increasingly paired with other aspects of user identity such as patterns of user behaviour during the online journey.

“If a (fraud) ring opens 100 accounts we can catch that,” said one merchant. “Our bigger concern is if an individual or small group figures out a better way to make things look legitimate.”

81% are concerned about new attack types emerging before the technology is available to fight them.
Automated intelligence and proactivity

78% of participants are concerned about the increasing volume of data breaches leading to more fraud, and 81% of respondents are concerned about new attack types emerging before the technology is available to fight them. Many respondents felt that, whatever shape fraud takes in the future, solutions that successfully combat it will have increased data assets combined with automated intelligence at their core, with manual review increasingly reserved for the most complex cases.

It is also clear that, as things stand, the Boards of many businesses still react to the risk of fraud only after an attack has occurred. Yet, fraud teams are highly aware of new threats and the technologies available to fight them. Most businesses would benefit from working with their fraud teams to introduce appropriate new technologies, sooner rather than later – in other words, before not after the fraud occurs.

Fraud and the user experience: different perspectives

It’s really positive for consumers that the payment industry is offering ever-more streamlined ways to pay. However this can pose a conundrum for those preventing fraud, who rely on data points to assess a transaction for risk. 79% of respondents felt that the shift to frictionless payments will lead to greater tension between the needs of user experience teams and fraud teams.

One obvious tactic is focusing real-time checks on data gained without user interaction such as device or historical data linked to that individual. While there was no clear consensus on how this tension between the UX (user experience) and fraud teams will be resolved, it is likely that registration and the initial loading of the payment instrument will become increasingly important interactions with the user.
Many current concerns

Although on an individual level Fraud professionals have a keen eye on future risks, their businesses remain most interested in the here and now. As such many respondents emphasised the immediate risks stemming from business activity such as new geographical markets, new product ranges and new ways to pay, with one respondent citing in particular the use of debit cards in Brazil. When taken together, growth in day-to-day complexity plus new unforeseen threats, present a major challenge for merchants as we move into the future.

Payment innovation - fraud evolution

New technology in payments emerges constantly, with the “Internet of Things” and invisible payments being two key current trends.

We predict more and more use of social identity as a valid means of establishing trust in a transaction, whether this transaction is peer to peer or a more conventional merchant-purchaser interaction. All this poses new risks particularly around the hijacking of identity.

Players in the industry are already responding to the need for robust management of online identity by creating centralised repositories of digital identity information. By entrusting online identity to one key player, individuals can remove the need to hold personal information with multiple organisations, and repeatedly authenticate themselves, instead taking a ‘one time only’ view. The key here is that one player or players need to gain sufficient market share to make this a reality.

“The future will be much more data-driven – the decision has to be a yes or no and move on.”