WORLDLINE

Fraud Risk Management for issuers and acquirers

Position Paper

Digital Payments
for a Trusted World

Fraud Risk Management

At a time when fraud is once again on the rise, both in terms of volume and complexity, with fraudsters becoming ever more ingenious and targeting new acceptance channels and means of payment, what should issuers and acquirers do to prevent, detect, and react to fraud, with a view to minimizing financial losses and the other negative impacts on their business or customers?

Are we on the brink of a new wave of fraud?

Fraud has become an on-going challenge for issuers and acquirers in recent years

After a period of decline and presumed stability, we are once again seeing an upsurge in fraud in Europe. The recent decline was mainly due to the migration to EMV which resulted in improved control at the physical POS. But, as ever, fraudsters are actively seeking out and exploiting the weakest links in the system, and the evolving digital economy has created new fraud threats and an increase in the number of financial crimes committed.

Fraudsters have now shifted from exploiting face-to-face to card-not-present transactions.According to the ECB, 60% of the total value of card fraud came from card-not-present payments (Card Fraud Report, Feb 2014). The majority of fraud is committed in the less-secure environment of electronic commerce, e.g. where merchants have not yet adopted 3D-Secure protocols and where issuers still rely on weak authentication methods or offer risky procedures such as activation during shopping. Countries most affected by fraud today are those with mature card markets with high e-commerce volumes (i.e. France and the UK).

At the same time, fraudsters continue to switch from cards to online bank accounts and credit transfers by gaining customers' credentials (using several criminal tactics including phishing and malware) and/or by directly infiltrating banking networks.

All of this suggests that we are once again on the brink of a new wave of fraud, and all the players in the value chain will be affected.

The typical situation for issuers

At a time when interchange is expected to fall, resulting in a decrease in a major source of revenues, any losses due to fraud, and the related costs, will hit your remaining margins hard.
It will therefore become increasingly important to fully understand the total cost of fraud:

•The direct costs of fraud represent the fraud losses themselves. This is the total amount leftover from payment transactions after clearing which were disputed by the cardholders and could not be charged back to any other party. This must therefore be written off by the issuer.

•The indirect costs of fraud are not always as obvious. They are mainly comprised of:

- Total costs of combating fraud: the cost of hardware, software and people associated with fraud prevention, detection, and reaction, and the subsequent operational follow-up; authentication and authorization; all investigations and dispute-handling (resolving and chargebacks,) whether managed internally or outsourced (partly or in full); and all of the related administrational efforts. Of course, here it is important to achieve the best possible results in relation to the investment made. Operational efficiency is key to avoiding inflationary effects.

- Cost to reputation due to late or undetected fraud cases. Indeed, image and reputation require a solid and consistent, yet credible, storyline for effective communication with your consumers. Negative press cannot be avoided by pretending that the fraud problem doesn't exist! Products supporting the active involvement of cardholders in the decision-making process may help to build and maintain customer confidence.

- The costs associated with rejecting genuine transactions due to decisions based on false positive detection results must not be underestimated. Needless to say, it is vital to detect as much fraud as early as possible (ideally prior to authorization approval). Yet, declining genuine transactions always leads to frustration; quite often this occurs with sensitive consumers who exceptionally use their payment products outside their standard behavioral patterns when they are at their most vulnerable emotionally (e.g. while travelling). Once cardholders lose trust in certain payment products, they are more likely to use others in the future. Therefore, real-time detection rules and models must guarantee very low false positive rates so that you are able to make informed decisions.

Fraud Risk Management is a strategic issue for you, the issuers and acquirers

While fraud poses challenges for all players in the payment value chain, the composition of total cost of fraud varies significantly, both from an issuing or an acquiring standpoint.

The typical situation for acquirers

As an acquirer, you may often find yourself caught in the middle between the conflicting objectives of different stakeholders, such as those of merchants and payment schemes, while all the while needing to keep an eye on the risk of your own exposure to fraud.

Payment schemes impose ever more stringent directives in order to protect their businesses and brands, and you are therefore expected to monitor your merchants.

- Acquiring in sectors such as dating and gambling, for instance, requires more stringent registration, reporting and monitoring than other activities.
- Contracting with merchants who offer new products which are attractive to fraudsters, including BitCoins and prepaid cards, also significantly increases the risk of fraud and thus the level of monitoring expected from you, the acquirer.
- You need to identify fraudulent merchants and those who are running illegal e-commerce businesses. Indeed, the fraud losses sustained from those merchants, who will have disappeared long ago with the money, will end up on your bottom line.

At the same time, your merchants are not fully aware of the threats they are facing, and expect more and more support from your side in this area.

Against the backdrop of a new wave of fraud, the risk of facing greater cost and reputational damage increases for both issuers and acquirers. Since trust is one of the pillars on which the digital economy relies, you have to put in place adequate measures for the prevention and detection of, and the reaction to, fraud!

What do issuers and acquirers need to do now?

1 Time to re-assess the situation

Now is the time for issuers and acquirers to re-assess their situation in order to take stock of all of the relevant processes, tools and measures they already have in place. These may have delivered good results in the past, but are they enough to cope with the new fraud wave (which may impact all channels and new products)?
Has the target been correctly defined?

Here are a few questions to consider:

Infrastructure:

Does your current hardware and software have limitations (volume, speed, etc.) which might have a negative impact, or are they easily scalable? How advanced are your current detection methods (do words like "machine learning" or "artificial intelligence" mean anything to you, or do you still rely on 20th century technology)?

Scope of your solution:

Is your solution also protecting your online banking? Do you use different solutions or methodologies for individual payment channels? Do you have an integrated solution in place which covers all payment channels and is more useful to your organization?

Organization:

Can you ensure adequate training and staffing of your expert teams if operational volumes were to double overnight? How scalable is your organization? Does your governance process deliver adequate reporting methods and monitoring of achieved results?

Overall fraud performance:

How are your KPIs looking? You might consider a detection rate of above 80% as acceptable, but what would you need to do to improve this to a figure above 95%? Furthermore, how quickly do you detect fraud? How often do you benchmark your results against those of your peer groups in your market? What is your fraud-to-sales ratio?

Communication with cardholders and merchants:

Do you actively involve cardholders when defining the individual usage limits of your products? Do you organize awareness-raising training sessions with your merchants?

2 Time to act

Having carried out a more detailed assessment, you could suggest that your organization decide on adequate and appropriate actions, e.g.:

- upgrading your existing tools and processes,
- asking for external support for advanced fraud management services,
- or even considering outsourcing fraud risk management to an external provider

Several fraud detection solutions are available on the market that can help you improve the level of accuracy in identifying financial crime events and increase your detection capabilities.

However, as fraud becomes radically more complex, we believe that offering a "one-size-fits-all" approach, with static and slow-changing intelligence used to examine suspicious behavior across huge numbers of transactions, is no longer sufficient in combating fraud.

The constant need for greater flexibility and high-alert data accuracy can only be provided by an intelligence-based approach which links monitoring technology – both real-time and post-authorization – with business expertise and strong workflow capabilities, complemented by strong governance to support effective investigations.

On this basis, you will be able to select and customize the most appropriate solution for you, which will deliver the following benefits:

- A balance between high detection rates and low false positives, in line with your appetite for risk
- Chargebacks brought under control
- Strong image of trustworthiness and security
- Improvement of other services such as credit risk management, anti-money-laundering, marketing (i.e. to enrich customer knowledge, increase sales and propose tailored services to customers) by leveraging fraud analytics and big data methods
- A more efficient fraud risk management thanks to a consistent interconnection between the different solutions applied to all payment means across all channels
- And finally, maximization of your revenues.

And to support you, for more than 40 years, Worldline has designed and deployed a powerful fraud-fighting strategy. As a result, we offer services, tools and fraud experts covering the entire Fraud Risk Management value chain.

About Worldline

Worldline [Euronext: WLN] is the European leader in the payments and transactional services industry and #4 player worldwide. With its global reach and its commitment to innovation, Worldline is the technology partner of choice for merchants, banks and third-party acquirers as well as public transport operators, government agencies and industrial companies in all sectors. Powered by over 20,000 employees in more than 50 countries, Worldline provides its clients with sustainable, trusted and secure solutions across the payment value chain, fostering their business growth wherever they are. Services offered by Worldline in the areas of Merchant Services; Terminals, Solutions & Services; Financial Services and Mobility & e-Transactional Services include domestic and cross-border commercial acquiring, both in-store and online, highly-secure payment transaction processing, a broad portfolio of payment terminals as well as e-ticketing and digital services in the industrial environment. In 2020 Worldline generated a proforma revenue of 4.8 billion euros.

worldline.com

For further information
sales-fs@worldline.com