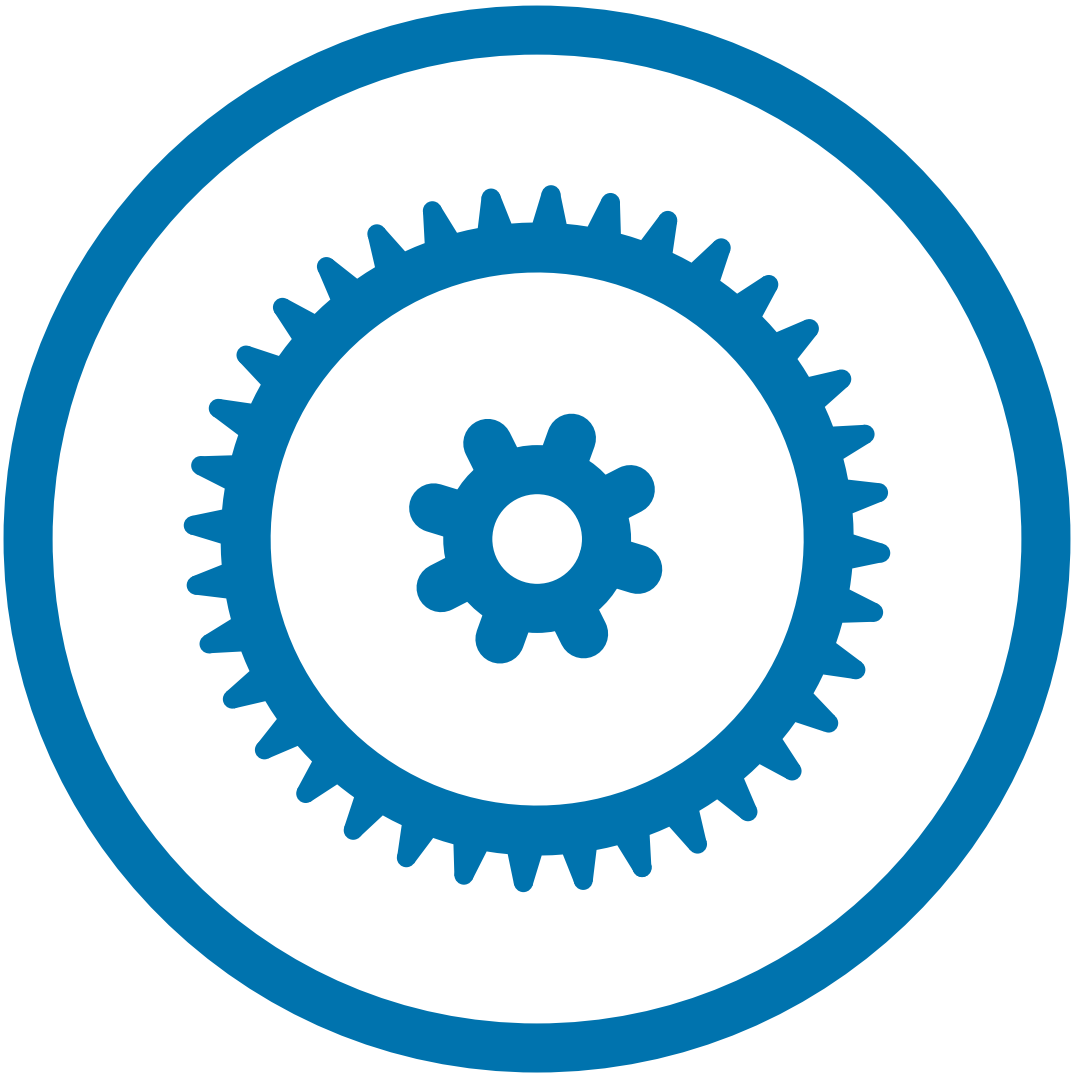
White Paper

acquirers

secure your business against merchant fraud



worldline
e-payment services

an atos company

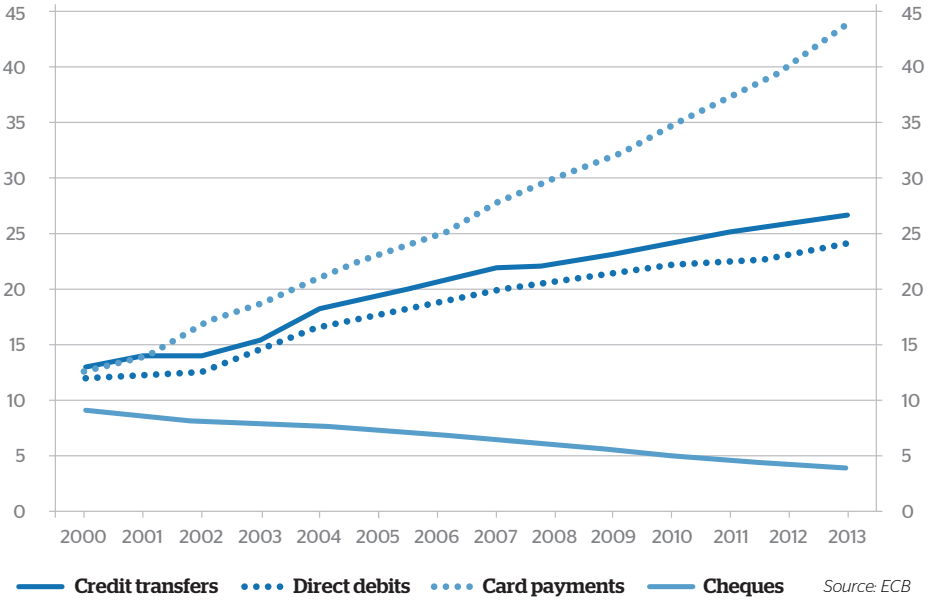
Acquiring, a market at risk

Acquirers should seek to retain and support existing merchants with improved services while asserting attention to areas where risk is present and where losses may be prevented.

With increasing demand for its services, acquirers are in a growth market where card and electronic payment continues to replace cash and checks.

Even in a transforming market with growing internet trade and alternative payment means, the traditional credit and debit card still remains the most used instrument for electronic payment. With increase of prepaid cards, mobile acceptance and micro-payments from emulated cards, a continued growth in electronic payment is expected.

ECB payment statistics for 2013



Source: ECB

Although acquirers are comfortably positioned in the payment landscape, it is also a position that is not without challenges. Increased competition from new entrants; Impacts from new EU regulation; Merchant insolvency rates higher than usual; Criminals and collusive merchants seeking to defraud and exploit the acquiring relationship, are some of those challenges facing acquirers in the current environment.

With the growth of E-payment, new players have emerged and entered the acquiring market with strain on profits and increased competition as a result. Under such conditions, mitigation of cost and losses from fraud and insolvent merchants can no longer be compensated through higher processing fees. Instead, to make their business more viable, acquirers should seek to retain and support existing merchants with improved services while asserting attention to areas where risk is present and where losses may be prevented.

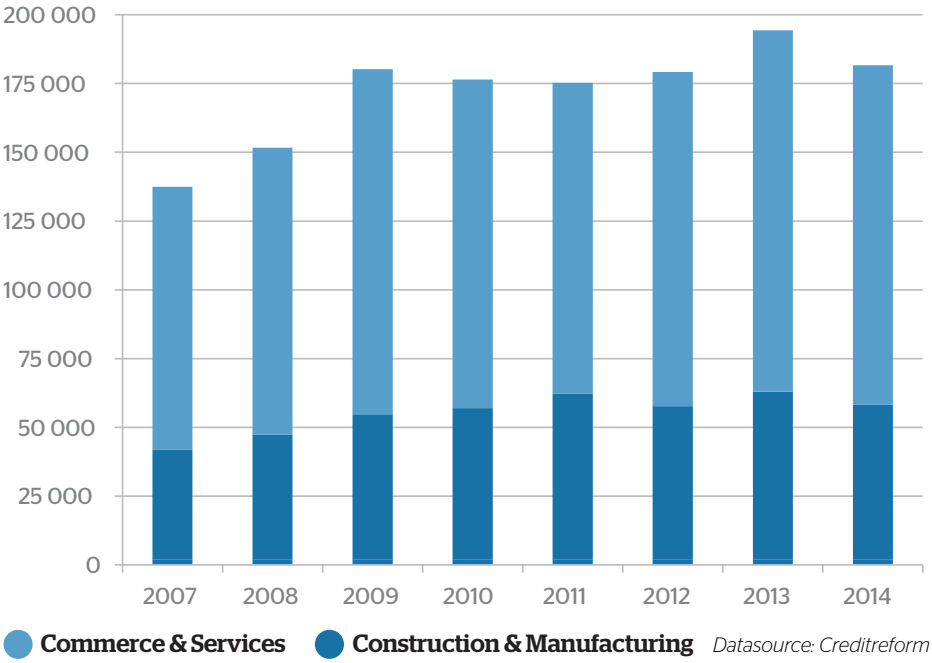
The greatest risk an acquirer is exposed to comes from its liability to compensate issuers and card holders, when merchants, due to insolvency or planned fraud, no longer can or will fulfill their chargeback obligations. It is a liability that is contingent and is carried for as long as 180 days after the transaction date.

In today's economic environment, with a higher than normal merchant attrition rate, it is therefore essential to have mechanisms in place that continuously scan and monitor for signs of merchant distress so that mitigating measures can be taken.

Actual and declared merchant insolvencies pose an immediate concern for acquirers. However, from a fraud perspective, the number of merchants balancing on the verge of insolvency represents an even greater concern, as merchants in distress are more likely to resort to fraud.

With chip-and-pin technology successfully having secured the card-present environment and 3D-Secure implementations continuing to secure the Card-Not-Present (CNP) environment fraudsters are becoming ever more imaginable and are increasingly resolving to 1st party merchant fraud.

Corporate insolvencies in EU15 +Norway, Switzerland frin 2007 to 2014



Datasource: Creditreform

As fraud has become more digitally orientated and its profit potential recognized by organized crime, an ecosystem of criminals has emerged. From sophisticated hacking and IT proficiency to merchant impersonation and physical presence when picking up the proceeds from e.g. a hacked ATM, individuals are teaming up and gangs are being orchestrated. Risks and threats that must be seriously considered by acquirers that consequently find themselves in a double role when servicing their merchants. In one capacity they need to service and protect their good merchants while in another, protect themselves, monitor and exert vigilance to merchant activities with fraud potential and other damaging effects, such as violation of card schemes, anti-money-laundering and PCI DSS regulations.

Critical signing policies in combination with in depth risk assessment and due diligence processes are first steps towards minimizing the exposure to fraud. **However ongoing attention to merchant activities and transactional patterns is even more important, as once on-boarded, the merchant represent a liability as well as being a potential source of and a victim to fraud.**

While the victim role carries no immediate risk for the acquirer, unless it leads to insolvency, and there are no formal obligations from card schemes to protect the merchants, the acquirers' position in the payment landscape makes it an obvious candidate for supplier of fraud protection services to merchants.

With increased competition and growing demands from merchants, acquirers have both a commercial and a merchant retaining interest in providing fraud related and other services, such as 3D-Secure, address verification and tokenization, in addition to core acquiring functions.

Each acquirer's situation and exposure to the above challenges is unique, depending on its specific environment and the level to which core acquiring and risk assessment capabilities already have been optimized. Regardless of which adaptive measures that may already have been taken, the underlying business and revenue model for acquirers remain the same. It is an imbalanced model where profit is generated as the sum of accumulated small transaction fees but where losses are counted in full, or pro-rata, share of transaction amounts. **Per definition, the Acquiring business model is sensitive to extraordinary losses from fraud and unexpected costs from card scheme fines and incompliance.**

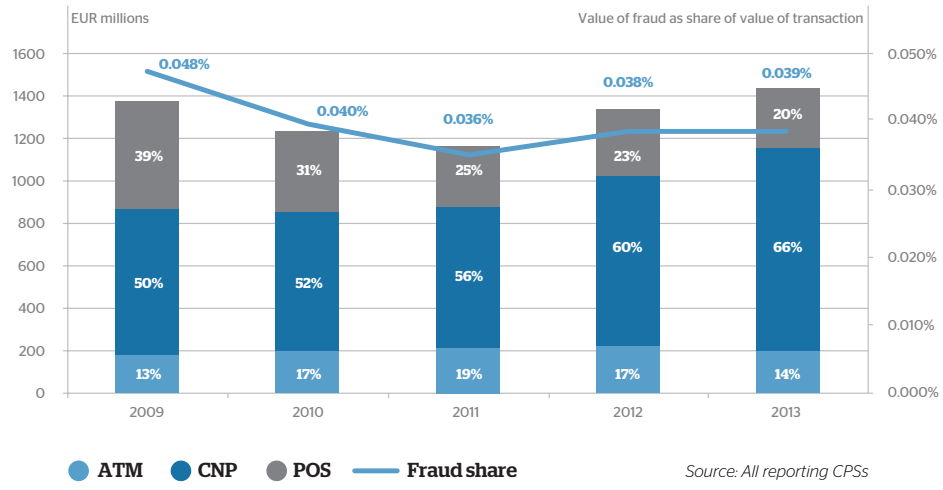
While challenges from increased competition and insolvencies are common and more or less affect acquirers to the same degree, the increased challenge from merchant fraud is one which the individual acquirer is better positioned to proactively control and mitigate. With the right tools, the right people and an organization vigilant to the topic, it is a challenge that, if addressed properly, can be a differentiating factor and a significant contributor to overall improved competitiveness. With that in mind, **the aim of this paper is to investigate the topic of merchant fraud, uncover how it is committed and how it most effectively can be mitigated**.

Acquirers risk from merchant fraud

Most detection of merchant fraud relies upon proactive, and near-real-time monitoring.

Monitoring of merchant web sites and sales conditions, should be conducted on a regular basis to detect unusual sales campaigns and promotions.

Evolution of the total value of card fraud using cards issued within SEPA



Source: All reporting CPSs

From 2008 to 2011 fraud losses in the EU area were steadily declining. In 2012, overall increases in Card-Not-Present fraud outweighed the positive effects from EMV and 3D-Secure implementations.

With continued roll-out and public embracement of 3D-Secure and other innovations, e.g. dynamic Cardholder-Verification-Codes, the incline is expected to be temporary. It is an expectation confirmed by more recent numbers for select countries. E.g. in 2014 the French organization 'Observatoire de la Sécurité des Cartes de Paiement' released a report, showing that fraud numbers peaked in 2011 with 0.341% of transactions being considered fraudulent. In 2012 and 2013 the numbers respectively fell to 0.290% and 0.229% which year on year represents a decline on 17.5% and 21.0%.

As both the Card-Present and the Card-Not-Present environments continue to be secured, fraudsters will attempt to target and penetrate the payment arena from different angles whereof the acquiring path is one.

The acquiring role is governed by the card schemes, setting forth obligations, requirements and thresholds for both acquirers and merchants. Obligations exist, from "signup" to "termination" including ongoing requirements for risk and fraud management. They constitute the minimum requirements for licensing and operation and are supplemented by optional recommendations, best-practices and self-assessment guides.

In some cases, obligations are described in detail, with the mandatory actions and measures, required to achieve compliance. In other cases, they are less explicitly defined, leaving room for acquirers own implementation, providing the obligations are verifiably met. As such, it is to a high degree the fraud fighting capabilities of the individual acquirer, and the extent to which recommendations and best practices have been followed, that makes the difference between adequate and outstanding acquirers.

If fraud is managed effectively, losses will be reduced. Instilled confidence, from strong fraud prevention and detection measures, will position the acquirer to target merchant segments with more profitable fees structures.

As sales channels and purchasing habits increasingly are digitalized, fraud scenarios are becoming more sophisticated and are ever changing. With such dynamics, and in order to respond efficiently, acquirers will depend on flexible and configurable IT systems to maintain the effectiveness of their fraud risk management solutions.

Data scientist competencies, in the areas of data mining and transaction analysis, are essential for a good solution. Considering the vast number of transactions processed, such capabilities are mandatory for early detection and reaction to real-time occurring abnormalities. In background mode, analysis on historic data, and in particular on data linked to actual fraud cases, can identify trends, similarities and other non-obvious patterns. Findings and outcomes from this analysis can be translated into new rules, and directly injected into a fraud detection engine.

Skilled and vigilant experts, able to react, and if necessary create new rules, from such findings, are an equally important factor to an effective fraud risk management solution.

In addition, throughout the merchant solicitation, due-diligence and risk-assessment phases, having experienced personnel in these domains also plays a vital role. Their accumulated unquantifiable experience, will contribute significantly to minimizing the acquirers' exposure and vulnerability to fraud.

Most detection of merchant fraud relies upon proactive, and near-real-time, monitoring of turnovers, transaction volumes and other characteristics, origin, brand, time etc.

Deviations and anomalies from normal transaction patterns and averages are regarded as indicators for potential fraud and will normally trigger an investigation.

If results, from such investigations, reveal nothing suspicious, a relaxed attention to the given merchant risks being the outcome, next time alerts from it are triggered.

However, continued surveillance should be exerted as sustained periods of lower than usual sales, and/or, sudden increase of sales, from discounting practices, could be indicators of a merchant in financial distress. The merchant may resort to drastic measures, which from an operational and transactional perspective are difficult to detect, but ultimately extends the acquirers' liability. Deep discounting (e.g. buy 1-get 1 free), change of 'Terms of Service' (e.g. postponement of delivery) could be ways of overcoming immediate cash flow problems.

Monitoring of merchant web sites and sales conditions, should therefore be conducted on a regular basis to detect unusual sales campaigns and promotions.

Bust-out merchants

It is important to have mechanisms in place capable of identifying unusual transaction and chargeback patterns.

"Bust-out merchants" denominates a type of fraud where criminals, through false applications disguise themselves as legitimate merchants, and where acquirers, from their contingent chargeback liabilities, bear the costs.

In short, fraudsters, with great effort and credibility, will approach banks and acquirers to setup accounts and an acquiring relationship for the sole purpose of generating transaction volume, collecting the revenue and run away sooner than the acquirer can discover and react.

Before the scam can be executed two pre-requisites must be in place:

- A legitimate merchant identity with trustworthy credentials, credit worthiness and a plausible business model.
- A genuine, but dispensable, store front with a credible appearance and infrastructure

Depending on the fraudster's network, patience and willingness to invest in the scam, it can be carried out with greater or less complexity. The challenging part of the scam is to establish an inconspicuous history with the acquirer and escape initial vigilance exerted toward newly on-boarded merchants. The scam can be of short duration, with the aim of generating transaction volume as quickly as possible and then 'busting out'. Or, it can be of longer duration, by initially accepting transactions from cardholders in collusion with the fake merchant, thus establishing a good history with the acquirer. Once that has been done, transaction volumes are increased using falsely obtained or compromised credit card account numbers. This typically happens at the beginning of a month as it prolongs the period for which the scam can remain operational and undetected.

End-month, card holders begin receiving their statements and detect unrecognizable transactions whereafter the normal chargeback process begins. With the sudden upsurge of chargebacks the acquirer soon realizes that something is not right and suspends further settlements. However, by this stage the merchant will already have transferred previously settled funds, have disappeared, and left financial repercussions to be carried by the acquirer.

This type of fraud is typically masterminded by criminals with the necessary network and resources to plan and successfully execute it. Considering their professionalism and likely experience from previous scams, it can be difficult to expose a prospective bust-out merchant upfront. Therefore, conducting a careful and critical due-diligence prior to merchant sign-up is imperative and a crucial first line of defense. While attention to newly on-boarded merchants is important, the risk that an existing and good standing merchant, for desperate reasons turns into a bust-out merchant also exists.

Acquirers typically have a graduated due-diligence process that is more or less comprehensive, depending on the risk profile associated with the merchant's business model. Business models with immaterial service delivery and fluctuating transaction patterns, from seasonal or event driven sales are ideal, as spikes in transaction volumes are expected and a normal occurrence, behind which, a merchant bust-out attack can be disguised. However, as fraudsters are aware of the added scrutiny merchants are subjected to when choosing a model like that, they may attempt to assume a less conspicuous model to deflect attention. Consequently, even for less obvious business models, the assessment process should be designed and applied as if a prospective bust-out merchant could be behind the application. **In this regard, and beyond having a capable fraud and risk department, it is equally important to have a trained and vigilant sales force that already in the merchant solicitation phase, understands and can identify potentially risky merchants'.**

Although no process can guarantee detection, a thorough assessment of the merchant applicant can expose and identify those with questionable backgrounds or where further inquiries or documentation should be requested before deciding if an acquiring relationship should be established or not.

Assessment should try to verify the merchant's background, business model and physical aspects of the business.

- e.g. are merchant and key personnel's history and records checked in company formation, insolvency, criminal and fraud registers?
- Does the merchant demonstrate true business knowledge; are expectations of transactions volume and turnover realistic?
- Are supply, manufacturing and delivery channels documentable? Are store or office premises and utility bills verified?

Should a bust-out merchant successfully manage to trick and deceive the assessment procedure it is equally important to have mechanisms in place capable of identifying unusual transaction and chargeback patterns. Early detection and containment of the attack is crucial. Fraudsters will continue exploiting the opportunity until effectively stopped. Alerts and suspension of automatic settlement procedures may limit impacts but unrecoverable losses may sometimes be unavoidable.

In a specific case, fraudsters had created an E-business, for rental of camp-site holiday homes on the Mediterranean coast, where customers were required to pay an advance deposit upon booking. Fundamentally a shrewd scam, as the web-site was easily implemented using captured photos from genuine camp sites. By choosing a business model with late-delivery as its nature, the scam would only be detected in the spring when customers would start heading south to camp and enjoy the warm climate. However, from lack of dedication to the scam, by failing to respond and communicate with customers after their bookings, an excessive number of chargebacks were recorded. Investigations quickly identified the merchant as a bust-out fraudster, who progressively had re-transferred incoming funds to a different account. Although losses were moderate, the case demonstrates how easily a scam from a business model with an immaterial and late-delivery service can be exploited.

In the given case, the fraudulent merchant was boarded from a different geographical area than that of the acquirers' traditional one. It had been solicited by a local independent sales agent. This also demonstrates the risk of using third party sales forces for merchant solicitation as their priorities not necessarily are the same as the acquirers'. So, although liberalization has opened up new markets and expanded the potential merchant base, it carries the risk of attracting merchants with questionable intents. If differences in business practices or language impede normal screening and risk-assessment processes, there is a greater need and incentive to carefully monitor newly on-boarded merchants.

Considering the bust-out methods fraud potential and the relative ease by which it allows determined and capable criminals to profit, it is one of the most serious threats acquirers are facing in today's market place.

Payment Facilitators

Acquirers should assess the adequacy of their organization and risk management systems to the extra dimension that payment facilitators represent in the classical acquiring model.

Payment facilitation originally emerged as a way for entities with a non-classical merchant background to benefit from the eco-system of payment. By assuming an intermediate role and undertaking processing capabilities on behalf of institutions such as e.g. the public sector and utility companies, a facilitator, as a registered merchant with an acquirer, could act as a gateway and provide transaction handling, billing, recurring payment and interfaces to proprietary IT systems.

Facilitators still play an important, although dwindling role, performing the above original activities. However, with E-commerce, online payment and consumer expectancy of payment per card in traditional cash and check environments, a new business opportunity and aspect of the facilitating role has emerged.

This role is referred to by various names: Payment service provider, Third party processor, Aggregator, Master or Super merchants, but with 'Payment Facilitator' appearing to have gained most widespread usage. Regardless of the name, the underlying nature of their service remains the same:

A gateway service, providing small-sized merchants the option to accept payment without a direct acquirer relationship and without the need of setting up a traditional merchant account with an acquiring bank.

Visa and MasterCard currently define small-sized or sub-merchant differently. For MasterCard the turnover threshold is one million dollars per year whereas Visa has a threshold of one hundred thousand dollars per year before the schemes require the sub-merchant to sign a normal merchant-acquirer agreement. Furthermore, at this threshold MasterCard, but not Visa, require that settlements must be done directly from the acquiring bank to the sub-merchant, thus, bypassing the Payment Facilitator.

A sub-merchant's reason for choosing to open an account with a payment facilitator rather than with a normal acquiring bank could be one or several of the following:

- Business is a personal and unregistered legal entity as normally required by the card schemes.
- Business has low transaction volume making it more attractive to pay per-transaction rather than paying a recurrent monthly acquirer subscription fee.
- Merchant has insufficient credit worthiness to obtain a true merchant account.
- Merchant business is considered too risky for a bank or an acquirers liking and an agreement is either not possible or only possible at disproportionately high cost.
- Merchant has a history and appears on a merchant black list file.
- More commonly, and at a more practical level, the facilitator is a supplier of another primary service to the sub-merchant and payment is offered as a secondary, but complementing, service e.g. web-hosting for online dating, gambling etc.
- Further, the payment facilitator may provide assistance with implementation of the payment interface or offer services such as analytical and marketing tools which a traditional acquirer does not.

As such, payment facilitators provide a legitimate and alternative acquiring option to small sized merchants, to entrepreneurs and to specialized businesses with limited turnover. Thanks to mobile terminals, the internet and E-commerce platforms, it has become possible to establish, or equip, an existing business with electronic payment methods being it a face-to-face or an E-business.

For acquirers, Payment Facilitators provide a cost effective way of gaining business and transaction volume without having to sign and onboard a multitude of new merchants. Considering that the administrative burden and cost from signing and onboarding a merchant, roughly is the same, regardless of its size but that revenue earning from these small-sized and low-volume merchants are limited, the incentives to sign them directly is low. By letting an intermediate entity manage the relatively costly signup and day-to-day management of the sub-merchants while only maintaining a single merchant relationship with the Payment Facilitator all parties benefit.

Card schemes recognize this model and today's rules and regulations are adapted accordingly, setting forth obligations and responsibilities for both the Payment Facilitator and the sponsoring acquirer. In short, and excluding the specifics in relation to turnover thresholds, the governing rules state that a Payment Facilitator undertakes the same obligations and responsibilities toward its sub-merchant's as an acquirer undertakes towards its merchants. While this distribution of responsibility principally provides a sound foundation for a delegated acquiring model, **the rules also state, that a Payment Facilitator is regarded as a merchant and that the acquirer is liable for all acts and omissions by a Payment Facilitator AND any of its sub-merchants. So, although the Payment Facilitator commits itself to screen and monitor its sub-merchants and their submitted transactions, the acquirer ultimately risks being subject to fines, having to implement compliance plans or have its acquiring status re-evaluated due to activities beyond its immediate control.** Excessive chargeback ratios, fraudulent activity, money laundering, signing of banned merchants or PCI DSS violations could be reasons for sub-merchant and Payment Facilitator misconduct that could reflect negatively on the acquirer's status.

Therefore, before any acquirer decides to offer its services to Payment Facilitators, it should consider these aspects and perform a self-assessment of whether its organization and risk management systems are adequately adapted to manage the extra dimension, which Payment Facilitators represent in the classical acquiring model. In example: how is alignment of assessment and risk criteria between acquirer and Payment facilitator ensured? Are existing merchant reviews and audit procedures applicable for merchants (payment facilitators) with processing capabilities? Are tools in place, e.g. web site monitoring solutions, to monitor sub-merchant activities with regard to sales of illegal goods, brand or other damaging activities? Does risk management system recognize sub-merchant transactions, chargebacks etc.?

Considering that the revenue model of payment facilitators is based upon fees from the number of transactions processed and interest earnings from retention of funds in the settlement process, there is an inherent business conflict with the card schemes imposed restrictions on turnover thresholds. When thresholds are surpassed, sub-merchants must set-up a normal merchant account with the acquirer. Furthermore, settlement must be done directly with the sub-merchant as mandated by MasterCard. For both the Payment Facilitator and the sub-merchant this imposes a disruption to their existing agreement and for reasons of either convenience or revenue retention, the practice of load-distribution is sometimes used as a method to circumvent the threshold rules. Load-distribution by the payment facilitator can be done by splitting transactions from one sub-merchant onto other sub-merchants accounts. Load-distribution by the sub-merchant can be done by spreading the transaction volume onto new sub-merchants accounts, which in fact are shell accounts with no employees or genuine operation. Both methods are prohibited and card schemes expect the acquirer to have procedures in place to monitor and detect such practices.

As with turnover, thresholds also exist with regard to chargebacks and fraudulent activity. To stay below threshold limits, load-distribution of above character may also serve as a circumventing method and in this context the acquirer is also expected to be able to monitor and have tools in place to detect such practices. Otherwise, in case of failure hereof, penalizing chargebacks, assessment of the acquirer or other disciplinary actions could be a consequence.

Third party acquiring

It is essential to have a vigilant dispute handling team paying attention to chargebacks that appear inconsistent with the registered business model of the merchant.

While Payment facilitators and other niche typed merchants, e.g. rental of terminals for fairs and other one-off events, fulfill a legitimate merchant role, other, more classic typed, merchants can also venture into the practice of accepting transactions on behalf of third parties. Whether it is being done through web-site redirection or from a displaced POS device, it is an illegal practice. It prevents both card holder and acquirer from knowing who they are actually doing business with. From the acquirer perspective it is particularly risky as the business or ownership of the third-party merchant could be one that would normally not qualify for a merchant agreement. A history of insolvency, fraudulent intent or selling of prohibited items could be reasons why a third party merchant would want to solicit, pressure, or pay, a merchant in good-standing to capitalize from an already established acquiring relationship.

Identifying merchants presenting transactions from a third party can be difficult. Sudden changes in turnover and/or transaction volumes could be possible first indicators hereof. A vigilant dispute handling team, paying attention to chargebacks that in some manner or form appear inconsistent with the registered business model of the merchant is essential.

Merchant collusion and accomplices

Identifying collusive practices is best done through pattern analysis and triangulation, looking for similarities between transactions that have already been reported fraudulent for CNP reasons.

With chip and PIN technology having been implemented and thus securing the card-present environment, card holder fraud is increasingly targeting card-not-present (CNP) environments such as E-commerce, mail-order and telephone-order.

While some incidents of CNP fraud are friendly, with an opportunistic true account holder being the perpetrator but claiming innocence, other incidents are committed by criminals using compromised card holder authentication data. Authentication data that may have been obtained through a fraudsters own engineering, e.g. hacking, or from accomplices somewhere in the transaction processing chain.

One source for compromised data is merchants, or their employees, who from reselling or cooperation with fraudsters become collusive to fraud.

CNP fraud, which, if executed on a grand scale by a gang of fraudsters in a bust-out scam, may have serious repercussions for any acquirer. Even on a small scale, when directed at a merchant struggling to remain solvent it can have serious consequences. Not only does the merchant suffer from the cost of lost goods he also carries the chargeback compensation liability and incur a chargeback fee from the acquirer.

The pre-requisites for CNP fraud can be as minimal as an account number, an expiration date and a card verification number. This information has therefore become much sought after and highly rewarded, when traded on the darker side of the internet by so called 'Carders'. When information is enriched with brand, card holder name, address and zip code, as the merchant source is in a unique position to do, the information becomes even more valuable.

Detecting the actual handover of information is impossible and acquirer's chances for identifying collusive practices is best done through pattern analysis and triangulation, looking for similarities between transactions that have already been reported fraudulent for CNP reasons. If card numbers in such transactions appear to have a common history of having been used at the same merchant, there is a possibility of either a collusive behavior or an insecure infrastructure, allowing third party access to what should normally be secure data. While the latter possibility can be established and rectified through an audit or an inspection, the first possibility can be more difficult to prove. However, even if concrete proof may be difficult to establish, direct contact to the merchant, and employees, will demonstrate the acquirer's vigilance which in itself, has a preventive and deterrent effect. In other cases with e.g. a consistent overlap of transaction timestamps and the work schedule of specific employees or e.g. a delivery address coinciding with that of an employee, evidence can be gathered and submitted to authorities for further investigation.

Successful triangulation at acquirer level depends on the number of merchants served and the number of CNP fraud cases the acquirer have visibility of. If the data set is limited the identification ratio will also be. Acquirers that are small or operating in a fragmented market space should therefore consider exchanging fraud cases with fellow acquirers to increase their possibilities.

Acquirers also need to be vigilant of fraud from merchants and account holders in collusion. Collusion that may be executed by presenting transactions from card holder accounts created for a bust-out purpose. That is, accounts where the account holder has no intention of paying the accumulated credit. Fraudsters will open an account, typically at several different banks, and after a period of normal and inconspicuous activity, apply for an increase of credit limits. Once obtained, a systematic shopping spree at a collusive merchant will take place. As proceeds from the factitious sales are received by the merchant, funds are divided according to a pre-arranged agreement.

Losses can be significant, as an estimated 200 million dollar scam involving complicit merchants bear witness of. In February 2013 the New Jersey district of the U.S. Department of Justice charged eighteen people in a scam involving creation of thousands of false identities and card accounts. Cards that subsequently were used at complicit jewelry merchants, where the proceeds were shared between the perpetrators.

Fraud of the above magnitude sometimes becomes public knowledge through filings or press releases whereas other, less significant, but still sizeable, scams remain publicly unknown. For reasons of image protection, ongoing proceedings or hope of recovery, acquirers may choose to report losses to charge-off, delinquency or credit-loss accounts rather than to a fraud-loss account.

While it typically is card holder authentication data being exchanged between collusive parties, merchant identification data is also an asset that can be of value to fraudsters. Using a compromised merchant or terminal id the fraudster may approach the acquirer pretending to be a legitimate merchant. Merchant identity theft like this can be used as a way of obtaining sensitive information or, with further social engineering, to open new merchant accounts benefitting from the legitimate merchants good standing with the acquirer.

Business-format change

The acquirer is mandated and required to conduct regular reviews of the nature of their merchant business.

As some goods and services are explicitly illegal and others considered so risky, that a merchant contract only can be obtained at comparable high fees and with collateral requirements. Some merchants may therefore be tempted not to disclose the true nature of their business.

Examples of prohibited goods and services: drugs, weapons, counterfeit goods, infringement of copyrights, and circumvention of product licenses.

Examples of goods and services considered high-risk and where ongoing review of the merchants' activities and financial soundness is required: adult content, gambling, pharmaceuticals, payment facilitation and uncommon charities.

Other merchants may attempt to set up businesses with a covert purpose of: money laundering, off-loading of stolen goods or the financing of illegal organizations. Careful signup and due-diligence processes are essential to prevent onboarding of ill-intended merchants. However, some may elude detection and others may transition from good to bad merchants. This is why continuous attention to change of business-format practices must be undertaken.

Regardless of the purpose for a format change, an acquirer risks being subject to fines and added regulatory oversight, resulting from breach of card scheme rules and failure to comply with e.g. anti-money laundering and terrorist financing laws. Further, an acquirer may suffer reputational damage by being associated with certain business types jeopardizing overall competitiveness.

Identifying a business format change is not done through one process alone. It is a combination of procedure and vigilance, that, together with ongoing monitoring, may detect indicators hereof. Once a merchant has passed initial due-diligence, has been boarded and operative without raising suspicion, most merchant contact is sporadic.

Exceptional events like changes to aggregates and / or transaction disputes may trigger contact. However, a merchant that, otherwise does not attract attention, and perhaps does it utmost not to, can therefore change its business format without it being observed.

For merchants in the high-risk category, the acquirer is mandated and required to conduct regular reviews of the nature of their business. However, regardless of business category, and as common practice when investigating alerts from unusual transaction patterns or aggregates, a change of business-format should be considered as a potential cause. Likewise, when investigating transaction disputes, attention to chargebacks and merchant responses that somehow appear inconsistent with the declared business format should give cause to a closer examination of the merchants' true dealings.

Changes to ownership, address and telephone number etc. are also possible indicators of a potential format change.

For merchants, with no or only basic, internet presence, such an examination may include contact, interview and inspection of merchant premises. For E-commerce merchants, with full internet exposure, a web-site inspection may also reveal business conduct changes or altered product offerings.

While performing the above examinations in alert and reaction mode, changes to business-formats may sometimes be detected proactively by employing a web crawling tool looking for e.g. redirections to alternative web pages or for specific revealing keywords. In one example, a drug selling merchant was identified by a web-crawler configured to look for slang words referring to marihuana.

False transactions

Acquirers should pay attention to unusual transaction patterns and put a closer fraud and risk analysis of the merchant in place.

Insertion of false transactions is typically done by merchants attempting to abuse the payment system or looking for ways of boosting turnover to overcome an immediate liquidity issue.

As 'profiting' method it has limited potential as cardholders in most cases will react and initiate a chargeback process, which eventually place the liability for the transaction with the merchant. Only in undetected cases or when the acquirer, on its own discretion, accepts liability for the transaction can it be profitable.

Consideration may be shown when the acquirer choses to authorize a transaction that under normal conditions would have been declined e.g. when issuers ACS were not responding, when there was a transaction timeout or when a blacklist was not consulted.

As turnovers are monitored constantly, and excessive movements trigger alerts, injection of false transactions can only be done on a smaller scale without being immediately detected. However, if done conservatively it may initially remain undetected. **This is why acquirers should pay attention to unusual transaction patterns such as the ones mentioned below.**

- Unusual number of declined authorizations indicating attempts to push transactions
- Unusual number of chargebacks for authorization reasons
- Unusual number of manually entered transactions
- Unusual frequency of the same account number in transactions
- Unusual number of first swiped and then key entered transactions
- Unusual transaction and batch capture time compared to business hours
- Unusual occurrence of even numbered amounts in transactions or batches
- Unusual number of transactions with amount exceeding normal average amounts
- Unusual transaction with discrepancies in authorization and clearing elements

If such patterns are identified, settlement payouts should be suspended and a closer fraud and risk analysis of the merchant put in place.

Another type of transactions, which should be monitored carefully, is credit / refund, transactions as they are interesting for a number of reasons.

With set card scheme thresholds for the monthly number of acceptable chargebacks before a merchant become subject to fines and extra scrutiny, the merchant may seek to resolve card holder disputes directly with the customer without involving either issuer or acquirer. Resolution may be done through credit transactions, so that a chargeback handling fee is avoided and the dispute case remains uncounted as a chargeback incident. **As chargebacks is an important instrument for both card schemes and acquirer's to measure the soundness of merchants, an unusual high number of credit transactions could indicate a habit of rule circumvention and obscure the true risk liability the merchant represent.**

Further, with credit transactions being comparable to money transfers, they provide a way of redirecting funds. Funds, that with todays' clearing speed, can be exchanged for cash within a day or two and therefore should be monitored actively to prevent them for being used fraudulently. The merchant itself may use them as a mean of withdrawing funds that would otherwise be regarded as taxable revenue. However, the most common exploit is seen from employees submitting credit transactions to own, or accomplice's, accounts. Examples exist, where false credits, submitted conservatively in terms of amount and frequency, over a number of years have totaled several hundreds of thousands euros before being detected.

Where merchants and employees previously were the source for falsified credit transactions, third party fraudsters now also use the method as a way of routing and siphoning funds from the payment system. From hacking, phishing or other social engineering fraudsters may gain access to merchant's IT-system or terminals and in that way submit false credit transactions to accounts owned by the fraudster or his accomplices. To mislead detection procedures, the fraudster may even in some cases have conducted a legitimate, lesser amount, sales transaction to justify the credit transaction.

To prevent merchants from being targeted, acquirers should actively educate and make merchant's aware of the risk from weak infrastructure, system credentials and phishing methods. Further, explain the risk which transactions from stolen terminals and unknown IP addresses might represent.

Should falsified credit transactions anyhow succeed in being submitted the acquirer should pay attention following indicators:

- Credit transactions without preceding sales transactions
- Credit transactions with amounts higher than original sale transactions
- Credit transactions to an account number different from the original sales transaction
- Credit transactions with amounts higher than average sales transactions
- Credit transactions benefitting the same account numbers repeatedly
- Credit transactions from stolen terminals with incorrect merchant name, terminal id etc.

If alerts from such indicators are received, transactions should be suspended from automatic clearing until manually investigated.

Keeping the upper hand in the fraud fight

Fraudsters are following the market trend: becoming more agile, leveraging the systems complexity to find new fraud technics, exploiting digitalization to invent new efficient tactics. Acquirers constantly need to adapt their prevention strategy and leverage technology to create flexible and powerful fraud fighting measures.

The challenges of fighting merchant fraud are ever increasing in all new forms of electronic payment and the risk of cost and reputational damage can be extensive for acquirers.

As trust is one of the pillars on which the digital economy relies, it is essential that acquirers increase their measures for the prevention and detection of, and the reaction to, fraud!

Acquirers often find themselves caught between conflicting objectives of different stakeholders, such as those of merchants and payment schemes, while they need to keep an eye on the risk of their own exposure to fraud. Payment schemes impose ever more stringent directives in order to protect their businesses and brands, and acquirers are therefore expected to monitor their merchants.

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

Several fraud detection solutions are available on the market that can help acquirers to improve the level of accuracy in identifying payment fraud and increase the 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 near-real-time – with business expertise and strong workflow capabilities, complemented by strong governance to support effective investigations.

It is of utmost importance for acquirers to re-assess their fraud situation, to take stock of relevant processes, tools and measures they already have in place. These may have delivered soothing results in the past, but have to be checked regularly to anticipate changes and opportunities that technological evolutions and fraudsters' ingenuity may bring to the acquiring arena.

With 40 years of experience and expertise beyond payments, Worldline is ideally positioned to support and contribute to the success of your acquiring business with optimized fraud control and detection services from professionals with a high degree of experience.

Worldline has designed and deployed a powerful fraud-fighting strategy.

As a result, we offer services, tools and fraud experts with an excellent fraud-fighting knowledge covering the entire Fraud Risk Management value chain.

You can rely on Worldline to successfully face the challenges of fighting merchant fraud.

About Worldline

Worldline [Euronext: WLN] is the European leader in the payments and transactional services industry. Worldline delivers new-generation services, enabling its customers to offer smooth and innovative solutions to the end consumer. Key actor for B2B2C industries, with over 40 years of experience, Worldline supports and contributes to the success of all businesses and administrative services in a perpetually evolving market. Worldline offers a unique and flexible business model built around a global and growing portfolio, thus enabling end-to-end support. Worldline activities are organized around three axes: Merchant Services & Terminals, Mobility & e-Transactional Services, Financial Processing & Software Licensing. Worldline employs more than 7,300 people worldwide and generated 1.15 billion euros revenues in 2014. Worldline is an Atos company.

Financial Processing & Software Licensing

Financial processing provides banks and other financial institutions with a comprehensive set of services to help them and their customers manage their cashless payments. Our services and innovative software solutions support the full range of card and non-card payments for acquirers and issuers. By combining our core services with a growing list of value-added services and full integration with in-house systems, we help our clients offer their customers a customised, profitable, secure, extensive and innovative product portfolio.

For further information
infoWL@worldline.com