Acquirers are vulnerable to merchant fraud in several different ways. Although many industry initiatives focus on fraud and identity theft, the reality is that a significant percentage of financial losses associated with credit and debit payments is the result of organized crime, business failures, inadequate monitoring of merchant accounts and financial loss from unfunded chargebacks.

Merchants may attempt to commit fraud in many ways, and acquirers need to be vigilant about many situations in addition to deliberate criminal activity. Fraudulent transactions, card scheme penalties for excessive fraud, and chargeback rates and real losses from collusive and runaway merchants all require merchant acquirers to have effective fraud and risk management programs in place. Some of the more common ways in which acquirers might be at risk from merchant fraud include the following:

- **Bait-and-switch criminal fraud.** Criminals may assume the temporary identity of legitimate merchants and enter into acquiring relationships for the sole purpose of committing criminal fraud.

- **Business format change.** Merchants that cannot gain approval to sell certain types of high-risk services or merchandise, or who might be denied a merchant account because they operate using a risky business format like multi-level marketing, often obtain merchant accounts by lying about the nature of their products or business practices.

- **Factoring.** Merchants sometimes accept transactions from a third-party vendor that cannot obtain its own merchant account. Factoring businesses require careful monitoring, as cardholders may not know or realize who the registered merchant is.

- **Fraudulent cards.** Merchants may attempt to defraud acquirers by knowingly submitting transactions using fraudulent credit cards.

- **Forced sales.** If merchants cannot receive authorization for a sale of a certain amount, say $500, then they may attempt to resubmit the sale at lower values until it is authorized — $450, $400, $350 and so forth. This type of payment processing requires careful monitoring because the acquirer can suffer the loss if the transaction is disputed.

- **Resubmitted transactions.** If transactions are declined because they are fraudulent, merchants might repeatedly attempt to submit the card over a period of days, weeks or even months with hope that at some point it might slip through the system.

Developing an effective merchant processing risk program is more art than science and often requires a bit of intuition and luck. No one set algorithm or methodology can be used to manage transaction risk. Discovering transaction fraud may simply be the result of a hunch sometimes, and at other times it may be based on years of risk-management experience. Each organization’s risk profile is unique depending on many factors, including merchant type, transaction volumes, technological resources and other criteria.
Moreover, an effective risk program must be dynamic and adaptable in order to combat the latest criminal tactics.

Suspicious patterns that merchant acquirers should monitor include the following:

- **Average tickets exceed the maximum ticket allowed.**
- **Daily/weekly deposit amounts exceed the maximum limit.**
- **Multiple authorizations exceed the maximum number allowed to a card.**
- **The number of declined authorization attempts exceeds the maximum.**
- **An unusual pattern of duplicated card numbers appears in batches.**
- **An unusual frequency of the same transaction values appears in batches.**
- **The same card number appears over a period of time in both swiped and keyed transactions.**
- **An unusual frequency of even values appears in batches.**
- **The batch is in an even numeral value.**
- **Refunds exceed debits in the batch.**
- **An unusual number of voids and refunds appears in batches.**

Acquirers should also closely monitor risky merchant category codes, e.g., airlines, hotels and eCommerce merchants.

Detection and prevention of the fraud scenarios mentioned above require various measures to be in place, including the following:

- **Transaction monitoring to detect sudden changes in transaction patterns; some examples of potential early indicators of fraud include earlier than normal chargebacks, higher than normal refunds and negative daily settlement amounts**
- **Monitoring techniques that analyze average transaction values, transaction patterns, chargeback reason codes, chargeback volume/timing and monthly processing that exceeds expected sales or an increase/decrease in returned sales (refunds)**
- **Detection for ticket amounts different than expected and different purchase patterns**
- **Detection and monitoring of accounts for an unusual increase in refund amounts**
- **Monitoring for the number of authorization attempts, multiple transactions to the same card and timing between transactions**

Merchant profiling is monitoring a merchant’s processing to guard against fraud and loss. Merchant profiling not only protects the acquirer but also the merchant and should be based on certain criteria and patterns. Some of the more common monitoring criteria include the following:

- **Processing limits.** The merchant is granted a monthly processing limit. This limit allows the merchant to accept credit card transactions up to that approved limit. The merchant’s processing volume is monitored throughout the month to ensure that the limit is not exceeded.
- **Average tickets.** During the merchant account approval process, an average ticket is calculated. This is the average of the prices of the product or service offered by the merchant. Any transaction that exceeds the average ticket is investigated.
- **Chargebacks.** The total number of chargeback, average percentages and reason codes should all be monitored for inconsistencies or anomalies. Chargeback patterns can provide insight to potentially fraudulent merchant activity.
- **Refunds.** Refunds are monitored to gauge possible loss. The refund percentage and values are monitored to ensure they are performed appropriately to reduce the potential for unnecessary chargebacks. This also ensures that fraudulent refunds are not issued. By combining refunds and chargebacks, an acquirer can estimate how much reserve may be needed to cover any potential losses.

- **Batch monitoring.** After each day’s processing, batch monitoring should include but is not limited to transactions that exceed the average ticket, excessive authorizations, and refunds and chargebacks.

ACI® CAN HELP

Processors and acquirers worldwide use ACI® solutions and services to mitigate loss associated with merchant fraud.
ACI Proactive Risk Manager™ for merchant fraud detection combines the pattern recognition power of neural network scoring technology and custom risk models with expert, rules-based strategies and advanced client/server workflow management software. ACI is the only provider of a risk-management solution for merchant acquirers that operates based on the acquirer’s individual historical fraud trends.

- **Proactive Risk Manager** enables an acquirer’s fraud and risk department to change and deploy rules and parameters as desired to detect or even prevent new fraud attempts. The solution allows all rules to be created, managed and deployed via a graphical user interface (GUI).

- **Proactive Risk Manager** is flexible and can easily interface with any acquirer authorization system; therefore, it can process any data element stored within the authorization message for fraud scoring, such as an eCommerce indicator. In addition, further data, such as risky terminal identifier numbers, can be loaded for targeted monitoring.

- All alerts generated contain a great deal of data and provide investigating analysts with full information — such as priorities, reason codes and filter mechanisms — to assess fraudulent activity.

- **Proactive Risk Manager** enables fraud and risk departments to monitor merchants in real time (in-flight authorization response checking), near-real time (just after the authorization) and batch mode. This potentially enables discovery of fraud more quickly, and in some cases can further mitigate fraud losses.

- Profiling through accumulated statistics, scorecards, neural networks and aggregates enables more detailed and accurate merchant fraud monitoring.

- **Proactive Risk Manager** segmentation features enable various merchant hierarchies or operating lines to be monitored within one solution, with different monitoring strategies. Portfolios, teams, rules and queues can be used to segment merchant monitoring.

When used in conjunction with ACI Case Manager™, **Proactive Risk Manager** can eliminate certain manual processes, such as manual re-key; it can also guide workflow process and aid in information sharing.

Workflow within **Proactive Risk Manager** guides and facilitates the various fraud investigation processes. **Case Manager** has configurable workflow to further automate associated processes and procedures within the department.

This paper was produced by ACI Worldwide®’s financial crimes solutions team. This highly expert team consists of fraud consultants from all over the world with years of hands-on experience in the fraud industry. More than 160 financial institutions in 46 countries have received guidance and support from the team through a variety of programs, such as fraud analytics, fraud prevention countermeasure strategy and departmental process engineering. To find out more information, please visit our website at www.aciworldwide.com.
ACI Worldwide®, the Universal Payments® (UP®) company, powers electronic payments for more than 5,100 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI® to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software solutions delivered on customers’ premises or through ACI’s private cloud, we provide real-time, immediate payments capabilities and enable the industry’s most complete omni-channel payments experience.