Driving Up Conversion with Effective Fraud Management

Building a fraud filter which supports genuine sales

ACI Worldwide
Real-Time Payments

Introduction

Two of a merchant's most important objectives sometimes work at cross-purposes: reducing fraud and raising conversion rates.

Fraud has a number of negative impacts on businesses beyond the obvious loss of goods and chargeback fees. Fraudulent purchases can also cost merchants in the form of penalties, wasted shipping costs and lost time dealing with chargebacks. In fact, research suggests that every dollar of fraud actually costs merchants $2.40[1] when you take into account all these additional factors. If fraud persists, merchants can also become 'risky' in the eyes of the credit card schemes and may need to pay higher transaction fees, or risk losing their merchant account altogether. The reputational damage resulting from fraud can cause a loss of consumer confidence, reducing revenues and customer loyalty.

With this in mind, some merchants build overzealous fraud prevention systems that place many genuine shoppers into the same bucket as fraudsters. As a result, perfectly good shoppers are insulted, declined and unlikely to return. At least one-third of shoppers declined due to a false positive fraud flag abandon their purchase.[2] Those false fraud flags have a significant impact on conversion rates and profits — with merchants leaving billions of dollars of revenue on the table in 2016 through overzealous fraud prevention setups.

The goal, then, is to find the balance that allows merchants to minimize fraud and maximize the checkout conversion rate, to prevent losses on both fronts. The previous paper in this series, Driving Up Conversion Rates in eCommerce, focused on how merchants can make their sales funnel as wide as possible, by offering a frictionless payments experience that captures high numbers of genuine shoppers. In this paper, we focus on how merchants can build an effective fraud filter for that sales funnel — one which is not so fine that it blocks genuine sales, nor so constricting that it impacts checkout conversion rates. It is all about stopping fraud and fraud alone, while facilitating genuine sales.

> "Setting up fraud management tools based on the specific factors affecting the fraud a merchant experiences, is the only way to properly balance fraud and conversion."

1 How to Filter the Fraudster

Building a Picture: Utilizing Big Data

Before evaluating the tools and processes best suited to building an effective fraud filter, it's important for merchants to first understand what their fraud looks like, what trends need to be catered to, and to recognize how fraud differs from genuine transactions.

The right starting point for this process is data. Using a wealth of data, merchants can build a picture of both fraudster and customer behavior to help establish the context for fraud management — to make sure that strategies and tools are effective in identifying fraud as well as supporting high conversion rates.

The data available through thousands upon thousands of transactions are a goldmine of information that can be used to combat fraud. The best data solutions dig deep into every transaction, gathering intelligence from every conceivable data point. Payment providers and merchants need systems capable of capturing and collating these massive amounts of data, enabling it to be analyzed for trends, even as those trends are still nascent or evolving.

The data one merchant gathers can sketch out patterns within their customer base, but critical to building rich intelligence is a good understanding of emerging fraud trends within and across market segments and geographies. This can only be achieved through constantly updating fraud management systems with information from both internal and external sources — including hot card files, chargeback data and information traded on the dark web. Fraud exchange services can also play a valuable role here — connecting merchants and issuers in a multi-directional information exchange that boosts the ability of all parties to make accurate and informed decisions. The richer and more intelligent data becomes, the more accurate, effective and efficient fraud detection strategies become, in turn reducing impact on genuine customers and checkout conversion rates.

The data available through thousands upon thousands of transactions are a goldmine of information that can be used to combat fraud.

Finding the Fraudster: Tools for Pinpointing Fraudulent Activity

Well-informed, properly implemented fraud management strategies will detect and prevent fraudulent activity quickly and efficiently. If set up incorrectly, or in a "one-size-fits-all" manner, conversion rates can be negatively impacted by the fraud prevention system. This is why merchants must properly evaluate the fraud tools available to them, select the right ones and configure them to suit their business and customer base.

Using the wrong combination of tools, or applying them in the wrong way, can make the fraud filter too constrictive, resulting in an increased number of false positive fraud flags and, in some cases, deterring genuine shoppers. Take 3-D Secure, for instance: it is a well regarded fraud prevention tool but, in certain markets or verticals, it can actually do more harm than good. Where consumers are unaccustomed to it (in Brazil and China for example[3]), using 3-D Secure can damage conversion rates by causing cart abandonment. In other markets, consumer endorsement means that the same tool actually improves conversion rates by reassuring customers about the security of their payment card.

Setting up fraud management tools based on the specific factors affecting the fraud a merchant experiences (such as business type, region, fulfillment options and sales channels) is the only way to properly balance fraud and conversion, by blocking fraud in ways that have little or no impact on genuine shoppers.

Fraud Indicator Tools

Traditional fraud indicator tools can work very effectively as part of an overall fraud management solution, helping to determine whether a transaction is likely to be genuine or fraudulent. But, as with our example of 3-D Secure, each of these tools must be evaluated and put to use only where it does not compromise the balance between fraud detection and sales conversion. There are many fraud indicator tools available to merchants, some of which — such as device fingerprinting and plausibility checks — rarely cause any issues for conversion rates. However, some do need more careful evaluation and configuration — below are a few examples:

Velocity checks

In payments, velocity is defined as the number of purchases coming from a specific origin. Thus, merchants can flag purchases if too many originate from a single account, entity or email address. Certain sectors can benefit from velocity checks more than others. They are, for example, a powerful tool for the airline industry to detect and prevent fraud. They are less useful in the telecommunications and gaming industries, however, because in those sectors such checks often decline many genuine shoppers.

IP geolocation

A shopper's location can tell you a lot about their intent, but it must not be judged in isolation. Comparing a shopper's IP address against other factors — such as BIN range or billing address — can detect discrepancies and flag those falsifying their address. Some cautionary measures should ideally be used with this tool, however — flagging suspect transactions for manual review rather than rejecting them outright, for example — to ensure there is no damage to the conversion rate.

Set limits

The larger the purchase, the larger a merchant's loss if it proves to be fraudulent. Set limits enable merchants to set monetary limits on the size of purchases. Yet, in certain sectors and during certain sales periods (such as new product launches or at peak trading times), it is important that transactions which exceed the set limit are not automatically rejected, instead introducing additional risk checks or being flagged for manual review to ensure that genuine sales are not lost. Whichever indicator tools a merchant selects, they must not only be aligned with one another, and with the business, but also treated as integral cogs in the overall fraud management strategy.

Case in Point: Combining Tools and Rules

MVNO Blocks Fraud and Maintains Rapid Growth

An innovative mobile virtual network operator (MVNO) offering a "pay-as-you-go" package to students needed to deploy an effective fraud management solution which allowed their inherently high-risk customer transactions, while blocking fraud.

A large number of students share the same post codes, which can cause issues for velocity rules. Students also commonly open new bank accounts and receive new payment cards at the start of the academic year, which can cause pattern detection tools to incorrectly identify them as fraudulent.

By using advanced IP information, the fraud prevention solution implemented by ACI could detect university IP addresses and adjust rules accordingly. Temporary modifications were also placed on certain rules to account for new student bank accounts being opened at the beginning of the year.

This approach has allowed the MVNO to continue its rapid growth and securely expand into a number of new geographies with high average acceptance rates, low chargeback rates and limited impact on fraud levels.

Key Findings

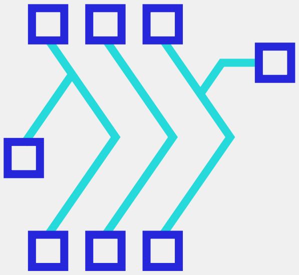
Rapid growth in last years

Expand into a number of new geographies with high average acceptance rates

Low chargeback rates and limited impact on fraud levels

Advanced Fraud Management Tools and Technologies

Just as fraud evolves so, too, do the tools available to detect it. Today, more sophisticated techniques are often being combined with traditional fraud indicator tools as part of a more holistic and effective way to manage fraud — using a multi-pronged approach to address a multi-faceted challenge.



Machine learning

Machine learning applies pattern recognition techniques to transaction data, from both fraudulent and genuine transactions, to build algorithms that can predict the probability of a transaction being fraudulent. These predictive models, with their ability to extract meaning from complicated data, can identify patterns too complex for humans or automated techniques to flag.

When machine learning models are correctly trained (using mass amounts of relevant transaction data) and configured correctly by experts, these techniques can be used to block fraud behind the scenes, invisible to shoppers, with no harm to conversion rates. By more accurately pinpointing fraud, machine learning models also help to support better conversion rates, by reducing false positives and ensuring genuine customers do not get unnecessarily declined or delayed by manual review processes.

Because machine learning models learn from experience, however, they can struggle to spot monolithic events, and can underperform when customer buying patterns suddenly move away from the norm. For this reason, it is important that machine learning, too, forms just one part of an overall fraud management solution — not only for optimizing fraud detection, but for protecting checkout conversion rates and customer loyalty.

A Leading Football Club Finds the Right Balance with Machine Learning

Concern that the fraud prevention strategy could impact customer sales during peak trading — with the launch of a new football kit — made a leading football club overly lenient with their fraud rules, allowing fraud to build.

Using three months of transaction data, ACI built a customized fraud solution, combining machine learning and tailored rules to provide a multidimensional approach to fraud prevention, with solution parameters that were specific to the risk profile of the club. These customizations were focused on finding the right balance between minimizing fraudulent transactions and maximizing genuine ones.

This tailored solution helped to reduce chargebacks to 0.22%, and manual reviews by 71%, giving the club the confidence to offer delivery of its promotional goods to nearly every country in the world.

Key Findings

Reduce chargebacks to

0.22%

Drop manual reviews by

71%

Delivery to nearly every country in the world

Tailored rules and alerts

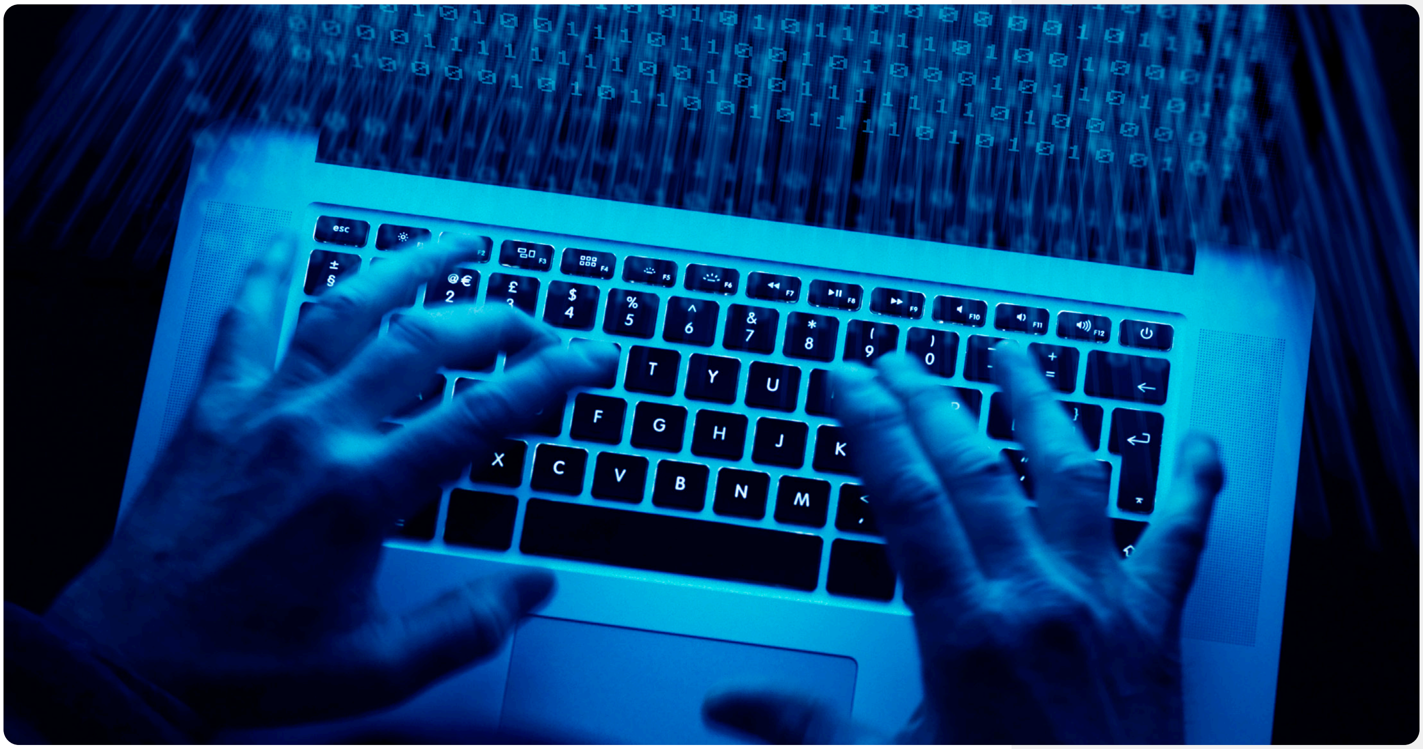
Combining pattern recognition capabilities with robust, flexible fraud rules can provide a powerful, optimized fraud prevention system which can be adapted to allow for emerging fraud and buying trends without compromising on risk mitigation or the customer experience.

The tailoring of fraud rules can start at a sector level to help with broad trends. For instance, in many sectors, fraudsters are most exposed at the time of fulfillment. Here rules flags can be used when an order is placed so the merchant is able to introduce extra steps, or checks, at the point of fulfillment, where needed. So, if a transaction hits such a rule, this might trigger a 3-D Secure check, the requirement for a signature on delivery or a call to the consumer to verify their purchase.

The available delivery options may also be limited. In this way, merchants can enable a smooth fulfillment experience for genuine customers while taking steps to counter the rising tide of fulfillment and delivery fraud.

Introducing fraud rules in silent mode to test performance and monitor higher risk profiles without directly impacting decline rates can also be a beneficial part of the tailoring process for merchants — especially during periods of growth or change. Profiles that are higher risk can be reviewed instantly using silent rule dashboards, creating layers of control through which emerging trends can be spotted, orders declined and refunds processed, removing future chargebacks. This is a relatively simple, but extremely valuable process.

...emerging trends can be spotted, fraudulent orders declined and refunds processed, removing future chargebacks.



2 Know Your Customer

Customer profiling

To balance strong fraud prevention and high conversion rates, an effective fraud filter has to be about more than just identifying the fraudster — it must have equal focus on positively identifying good customers. This is the only way that merchants can make sure their fraud management strategy treats genuine customers differently, to drive conversion, improve the customer experience and boost loyalty.

Many fraud management tools and processes can help use data to build fraudster profiles — but, with the right focus, they can equally help to build a rounded profile of genuine customers.

For instance, most merchants will have in place a black list which is used to help automate the fraud decisioning process. Information typically provided includes account details, email address, payments method or other specific categories. However, it is prudent to also build and use a white list within that same process, to ensure genuine customers are recognized and treated accordingly. One advantage of black and white lists is that they can be quite flexible, giving merchants various options on how to proceed. For example, a common method is to place suspected fraudsters onto a black list temporarily (often for 24 hours), which gives merchants immediate protection, but in cases where fraud is not confirmed, allows shoppers to try again.

Analytics and behavioral profiling capabilities can also be effectively used to positively identify customers and deepen understanding of customer buying trends and preferences. Sophisticated monitoring and reporting tools can illustrate developing fraud and customer patterns, and quickly highlight any impact that fraud management strategies may be having on them — whether good or bad. This allows merchants to quickly make changes to the fraud rules to protect against additional fraud losses, or to prevent any further dip in conversion rates. Analytics can also be helpful in supporting conversion rates where automation often falls down — for example with high-risk transactions. While high-risk shoppers are frequently automatically declined, with advanced analytics capabilities in place, merchants can instead accept these transactions and monitor the shoppers' subsequent activities, retroactively blocking any that are later identified as fraudulent.

> "An effective fraud filter must have equal focus on positively identifying good customers. This is the only way that merchants can make sure their fraud management strategy treats genuine customers differently."

Case in Point: Using Customer Data to Detect Fraud and Drive Sales

Reducing the manual review rate with the "time on file" tool

The in-house fraud solution at a leading retailer did not provide detailed customer profiling or analytics, resulting in a high review rate for online transactions, an overloaded manual review process and a high number of false positives. International cards and transactions weren't being accepted and the business was turning away customers from high-risk areas.

ACI worked with the merchant to analyze data and segment customers, behaviors and product sets by risk level. This analysis was combined with global pooled data from ACI to create a set of tailored rules which prioritized the merchant's genuine customers.

"Time on file" tools helped to support the customer experience and reduce review rates, while challenge rates and fraud rates fell significantly.

Key Findings

Challenge rates and fraud rates fell significantly

Support the customer experience

Catering to Your Customers

Gathering data, interpreting it and using properly tailored tools are all vital for effective fraud management, as well as for building a picture of genuine customers and ensuring they are not declined. However, there is a huge amount of extra value in taking this one step further, and using the intelligence gained from profiling activities to offer wider choice to genuine customers — to support higher conversion rates and increase customer loyalty.

By recognizing and marking genuine customers, merchants can offer increased flexibility and choice during the payments process. This could be in the form of offering different, higher-risk fulfillment options such as next- or same-day delivery, for example.

Another popular option is to implement "active payments method selection," which enables merchants to cater the payments method offering according to a shopper's risk profile. Safe shoppers are offered the entire range of options, while riskier shoppers are only offered more secure payment methods that often include additional risk checks.

It is also now becoming common practice to tailor authentication processes to fast-track loyal customers, to promote a positive customer experience and boost loyalty. For instance, larger merchants frequently now choose to let valuable genuine transactions circumvent 3-D Secure, to reduce the process by an extra step and secure the conversion more quickly.

By recognizing and marking genuine customers, merchants can offer increased flexibility and choice during the payments process.

3 The Human Connection

Automation is a wonderful thing. It is efficient and, if the parameters are properly set, usually highly accurate. However, even the very best automated systems benefit from human backup and one key element of this is the manual review process. Flagging transactions for review when certain pre-set conditions are met allows a fraud prevention expert to determine whether a transaction is genuine and should be allowed to complete. Manual review processes provide merchant fraud management teams with the flexibility to sift through the riskier, but not necessarily fraudulent, transactions, making incremental yet valuable improvements to the conversion rate without increasing fraud.

Outside of the manual review process, there is an even more vital role for fraud experts to play in the day-to-day management of fraud strategies. Almost every fraud management tool and process needs to be configured by experts to get the best value from it and to make informed decisions.

> "There is a vital role for fraud experts to play in the day-to-day management of fraud strategies. Almost every fraud management tool and process needs to be configured by experts to get the best value from it and to make informed decisions."

Also, where the fraud platform itself performs the majority of the analysis, experienced fraud analysts are able to focus on reviewing data and trends and taking steps to optimize platform performance. It is this constant monitoring and rule set adjustment that ensures fraud detection and conversion rates are managed effectively.

More than this, fraud experts can themselves become revenue enablers, by using their own knowledge plus the intelligence and tools at their fingertips to support broader areas of the business. Fraud management systems can be a source of very valuable intelligence for sales and marketing departments and, where information and business strategies are shared, fraud managers can help to support promotions and business growth, proactively preparing fraud strategies that cater for planned changes and monitoring performance throughout. They can also help to provide a valuable window to customer behavior and purchasing trends.

Case in Point: Expert Analysis to Support Better Decisions

Airline saves €3 million by reviewing existing rule sets
A European airline operator was experiencing fraud across a number of channels, especially website and call center. Last minute bookings were a major problem area, and many of these transactions were being conducted using U.S. cards. With 50% of the airline's transactions coming from international cards, the risk that the U.S. sales channel might be shut down by the card schemes represented a huge threat to the company's profitability and growth prospects.

Together, ACI's risk analysts and the airline's fraud team reviewed existing rules, analyzed historical transaction data, customer behavior profiles and fraud detection performance. Based on their industry knowledge, the ACI team was

Key Findings

97%

of all confirmed fraud was denied by the rules

Manual review rates reduced to less than

5%

Chargeback rates fell to less than

0.1%

able to recommend the addition of several new data fields to enhance the airline's fraud strategies — and a focus on critical issues, such as consistently prioritizing short-notice bookings in the fraud screening process.

In the first year of the collaboration:

- An average 97% of all confirmed fraud was denied by the rules, saving the airline €3 million
- Manual review rates reduced from 12% to less than 5%
- Chargeback rates fell to less than 0.1% on average

The airline has made a success of its U.S. sales channel and safely expanded into other geographies.

4 Conclusion

Building a holistic fraud management strategy which is configured to drive conversion rates is the way to keep sales moving safely through the funnel. The key to success lies in fine-tuning the fraud filter — not just as a net to catch the fraudster, but as a broader protective barrier against loss, whether that loss is in the form of fraud or reduced conversions, as both are equally damaging. This means tailoring and using a properly configured and aligned combination of tools, underpinned by expert support, a wealth of intelligent data and powerful analytics capabilities.

Ultimately, fraud and conversion rates do not have to work at cross-purposes. Merchants, and their payment providers, must recognize that their real goal is to identify and differentiate between fraudsters and genuine shoppers — blocking one group and supporting the other. It is important to remember that fraud management can help merchants to positively identify customers as well as fraudsters — to ensure they are treated differently and delivered a frictionless checkout experience which maximizes conversion rates. No other objectives are more important for a merchant's payment setup, and success means boosted revenues, higher customer satisfaction and, ultimately, increased profits.

> **"The real goal is to identify and differentiate between fraudsters and genuine shoppers — blocking one group and supporting the other."**

And lastly, fraudsters will constantly adapt to beat the system, while genuine shoppers shift preferences, try new ways to shop, act in unpredictable ways and expect more from each subsequent shopping experience. It is critical that merchants maintain dynamic solutions to prevent fraud and increase conversion rates. No solution, no matter how effective, can be set and forgotten and a merchant's approach to fraud management must remain fluid, informed, timely and adaptive to ensure revenues are protected.

[1] LexisNexis "True Cost of Fraud study 2016"

[2] Javelin Strategy & Research "Overcoming False Positives" 2015

[3] Edgar, Dunn & Co "Impact of 3D Secure on Transaction Conversion Rates" 2014

ACI Worldwide is a global software company that provides mission-critical real-time payment solutions to corporations. Customers use our proven, scalable and secure solutions to process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with local presence to drive the real-time digital transformation of payments and commerce.

LEARN MORE

www.aciworldwide.com
@ACI_Worldwide
contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ATL1158 04-21

ACI Worldwide
Real-Time Payments