



DOES YOUR FRAUD PREVENTION NEED A TUNE UP?

SOLUTIONS FOR THE
AUTOMOTIVE &
POWERSPORTS
INDUSTRY



 Fraud

One or more of these 6 signs may be warnings that your fraud prevention process needs a tune up. If you're seeing these signs, get it in for repairs now, before you get hit with big losses, higher expenses, and falling revenue.

6 Signs Your Fraud Prevention Needs a Tune Up	3
1. Higher Chargebacks	4
2. Increasing IT Complexity	5
3. Growing Product Losses	6
4. More Time Spent on Manual Reviews	7
5. Delayed Orders & Lost Sales	8
6. Avoiding New Markets or Opportunities	9
6 Strategies for Tuning Up Your Fraud Prevention	10
1. Superior Fraud Screening and Analytics	11
2. Real-Time Data Orchestration	12
3. Advanced AI Machine Learning	13
4. Expert Human Intelligence	14
5. Chargeback Alerts	15
6. Simple, Affordable SaaS	16
Avoid a Major Breakdown	17

6 Signs Your Fraud Prevention Needs a Tune Up

Are your profits headed for a breakdown? You've likely heard that the adoption of EMV (also called Chip & Pin) at point-of-purchase in retail locations is making card-present credit card fraud much more difficult and costly. You may be experiencing that this development is driving fraudsters to card-not-present (CNP) and mobile fraud, where EMV provides no security.

What's more, high-profile data breaches continue to make news – nearly 7 billion records compromised since 2005.¹ Then there's the dramatic rise of mobile commerce – predicted to reach nearly \$800 billion this year² – but which is also twice as likely to involve fraud as standard eCommerce, according to The Fraud Practice.³

The combination of these factors are why analysts are forecasting a perfect storm of fraud for online businesses, with **CNP fraud losses projected to soar 80%** to a record \$7.2 billion by 2020, up \$3.2 billion from \$4 billion in 2016.⁴

If you're a business conducting online eCommerce, you may be seeing signs of this fraud wave.

1. Higher Chargebacks.
2. Increasing IT Complexity.
3. Growing Product Losses.
4. More Time Spent on Manual Reviews.
5. Delayed Orders & Lost Sales.
6. Avoiding New Markets or Opportunities.
7. Escalating Training Time.

1. Higher Chargebacks

Creeping or soaring? Fraud is responsible for nearly 2 out of 3 chargebacks. You'll need to increase performance of your fraud prevention capabilities if you are experiencing:

- ⚠ Chargeback rates consistently in excess of 0.5%
- ⚠ Sudden or rapid rise in chargeback rate
- ⚠ Increase in overall volume and/or value of chargebacks (greater frequency and/or higher per-order costs)
- ⚠ Higher fees or increasing fines from your payment processor for chargebacks
- ⚠ Requirements from your payment processor to fund an escrow account to cover chargebacks
- ⚠ Alerts from your payment processor about being considered for an Excessive Chargeback Program
- ⚠ Warnings from your payment processor that they are considering terminating your merchant account



2. Increasing IT Complexity

Devoting more IT resources, budget and people to fraud prevention?

About half of eCommerce and mCommerce merchants say controlling fraud costs too much.⁵ IT is an area of particular concern. According to proprietary research conducted for Kount, most eCommerce operations worry about their lack of in-house integration resources and solution complexity. The following are signs that you may need to repair your current anti-fraud efforts:

- ⚠ Deploying additional ad hoc fraud prevention tools
- ⚠ Seeing an increase in the costs and people to manage tools
- ⚠ Increasing number of system integration projects as you attempt to unify disparate tools
- ⚠ Higher IT support and maintenance costs as complex anti-fraud, systems, and infrastructure require outside experts to maintain



3. Growing Product Losses

Lost and stolen products hitting your bottom line harder? The LexisNexis “true cost” of fraud as a percentage of revenue is more than 60% higher for online merchants than for merchants in general (online merchants = \$2.40 in true costs for every \$1 in fraud vs. all merchants = \$1.47 in true costs for every \$1 in fraud).⁵

What’s more, the higher the value of a transaction, the more likely it is to be fraudulent. In fact, a \$1,500+ order is 10x more likely to be fraudulent than a \$100 order.⁶ As an eCommerce operation, you need to look under the hood of your fraud prevention systems if:

- ⚠ Losses from stolen/lost merchandise are on an upward trend
- ⚠ You’re seeing higher Cost of Goods Sold (COGS) and reduced profitability
- ⚠ “Lost” shipping expenses are higher due to increasing chargebacks and fraud



4. More Time Spent on Manual Reviews

People are your most expensive resource. For most online businesses, the personnel costs for staff devoted to manual reviews make up more than half of their fraud prevention budget. Yet the vast majority of manual reviews are unnecessary, with an average of 75% of manually-reviewed orders being ultimately approved.⁷ Nonetheless, when chargeback rates start to increase, the typical reaction is to review more orders. Instead of defaulting to more manual reviews, it may be better to take a more comprehensive look at your fraud prevention efforts if you notice:





- ⚠ A higher percentage of orders being manually reviewed
- ⚠ Increasing staff time spent on manual review duties
more review agents to handle increasing review volume
- ⚠ Manual processes are the first line of defense, instead of the last



5. Delayed Orders & Lost Sales

Slow means “no.” Balky fraud prevention systems and drawn out manual reviews cost you sales. A 1-second delay in page response can result in a 7% reduction in conversions.⁸ Or to put it another way: if your eCommerce site is taking in \$5,000 - \$10,000 per day, you could potentially lose \$125,000 - \$250,000 in sales annually due to sluggish anti-fraud tools.

Delays caused by slow manual reviews are also a problem, leading to cancellations and even customers turning to your competitors. It's probably time to give your fraud prevention system the once-over if:





-  Processing time for your fraud prevention tools or system averages more than a fraction of a second
-  Customer transactions actually “time out” due to fraud prevention processing delays
-  Manual reviews average more than 30-45 seconds before reaching a decision
-  Manual reviews cause order fulfillment or shipping backlogs



6. Avoiding New Markets or Opportunities

You miss 100% of the revenue on orders you don't

take. About 2 out of 3 online merchants refuse to sell outside US borders.⁹ The number one reason? Fear of fraud from foreign shoppers.⁹ Of course, that's just one opportunity. If your anti-fraud system lacks enterprise-class capabilities, you may be avoiding new markets, new channels, or new products because the risk/reward equation tilts too heavily to the risk side. If so, then it's time to review your fraud system. You should consider an updated solution if you are:

-  Not listing certain items on your website because they are highly-targeted by fraudsters
-  Avoiding affiliate opportunities that could generate substantial traffic to your eCommerce website due to concerns about affiliate fraud
-  Not selling in "high-fraud" cities, regions or countries
-  Delaying rollout of mobile commerce initiatives due to concerns about higher rate of fraud in mobile transactions



6 Strategies for Tuning Up Your Fraud Prevention

Use the right tools. The following 6 strategies are proven to help your eCommerce operations improve profits and sales.

1. **Superior Fraud Screening and Analytics.** Analyze hundreds of data points per transaction, using multiple, integrated technologies to detect fraud.
2. **Real-Time Data.** Check borderline transactions against third party data and capitalize on Big Data in real-time to separate good transactions from bad transactions.
3. **Advanced AI Machine Learning.** Automate insights from Big Data to reduce manual reviews, cut operating costs, and approve more of your borderline—but valid—orders.
4. **Expert Human Intelligence.** Respond to adaptable human adversaries in ways that are best for your business.
5. **Chargeback Alerts.** Intercept “bad” transactions even after they’ve been approved, so you can avoid product losses and chargeback fees.
6. **Simple, Affordable SaaS.** Avoid IT integration hassles, minimize cost and complexity, and gain certainty over costs.



1. Superior Fraud Screening and Analytics

Analyze massive amounts of data. Multiple technologies that screen multiple dimensions of every transaction help reduce fraud, lower the number of manual reviews, and eliminate “false positives” (good transactions that only look suspicious).

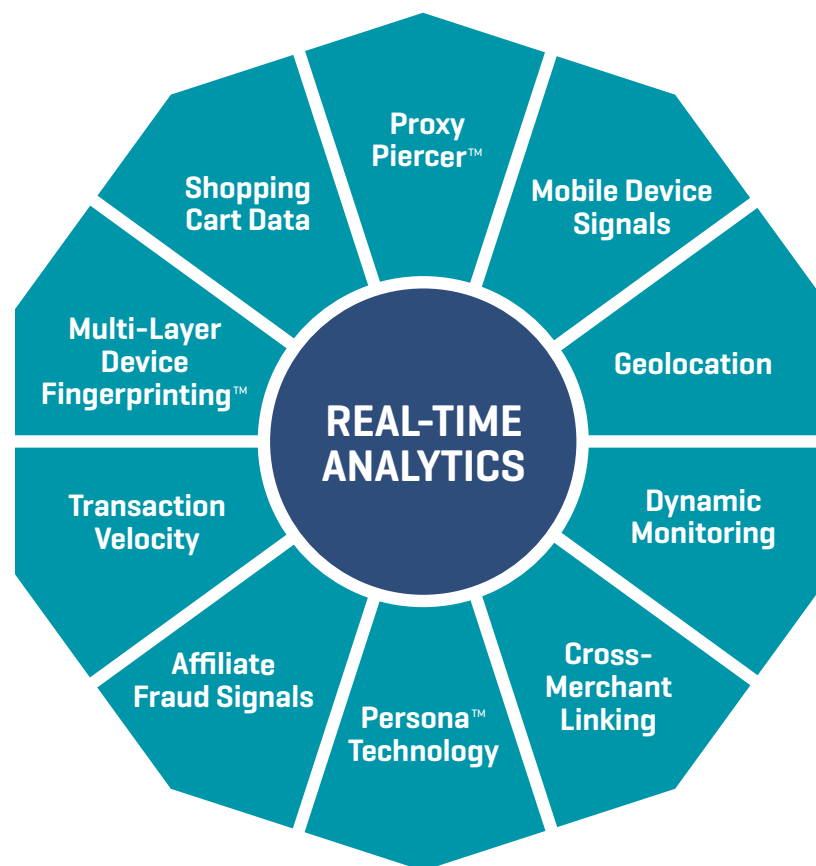
Multiple data elements per transaction. The more data analyzed—Device ID, Geo-location, Transaction Velocity, Order Linking, etc.— the more precise and accurate the screening.

Massive network effect. Behavior or attributes that might seem inconsequential within a small data set are revealed to be critical with Big Data analysis.

Integrated system. Individual data points analyzed by each technology informs the response of all other technologies to build a cumulative “picture” of the transaction for maximum fraud detection.

Real-time analysis in milliseconds. Fraud prevention should never slow down transactions or impede conversions.

Kount employs dozens of proprietary and patented fraud screening technologies—integrated at the code level—to generate hundreds of data analysis elements per transaction across billions of transactions from over 180 countries...all analyzed in under 350 milliseconds.



2. Real-Time Data Orchestration

Analysis informed by real-time data from best-in-class providers. When transaction data by itself is insufficient to precisely quantify risk, outside information sources can fill in gaps to provide crucial context, helping you distinguish good transactions from bad ones.

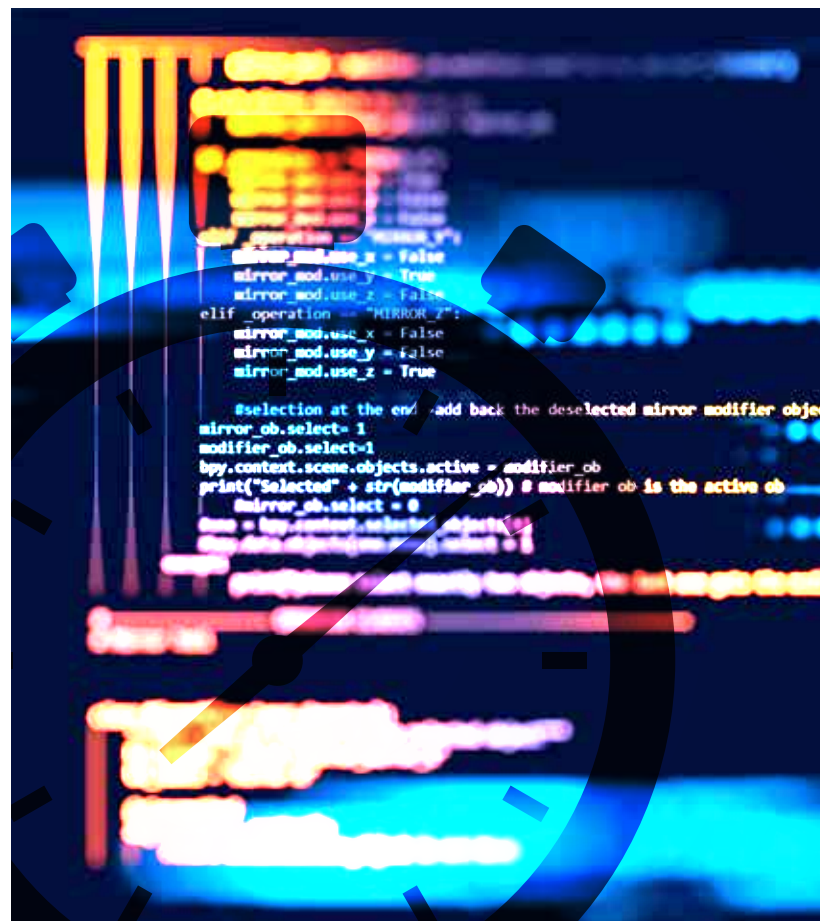
Integrated access to best-in-class information. Enhance insights by tapping into outside services...but only when necessary.

Orchestrate decisions based on your risk criteria. Give weight to factors based on your specific tolerance for risk, and fine tune your response to borderline transactions.

Single integration, multiple data feeds. The greater the number of information sources, the clearer and more robust the picture, resulting in enhanced detection.

Multiple and complex use cases. Clear-cut fraud is easy to detect. It's the ability to correctly evaluate borderline transactions that minimizes fraud losses while avoiding lost revenue due to false positives.

Kount orchestrates and integrates multiple best-in-class, third-party data sources to deliver optimal context for detecting and preventing fraud...but only on an “as-needed” basis to minimize data costs.



3. Advanced AI Machine Learning

Machine learning spots patterns in Big Data undetectable to humans. Go beyond just detection and prevention. Graduate to prediction and thwart emerging fraud threats.

Online learning. Extract highly predictive features in real time across the entire network to enhance fraud detection in low-information scenarios (e.g., first-time fraud).

Offline learning. Non-stop evaluation and refinement of AI results by human fraud experts ensure machine learning algorithms are continuously optimized.

Rules integration. AI and machine learning by themselves are not as powerful or precise as when they are complemented by a rules-based system for maximum control and transparency.

Kount's advanced machine learning uses patented graph theory algorithms (PERSONA™) to detect and respond in real-time to emerging threats...but according to rules you set to maximize revenue while holding down fraud.



4. Expert Human Intelligence

Best practices and the ability to respond to strategic, adaptable fraudsters. Rules set by thinking humans enable a strategic and customized response to rapidly changing fraud tactics.

Domain knowledge. Systems developed by fraud experts start with an inherent advantage over human adversaries.

Business-oriented. Instead of rules and thresholds being set to some generic technology standard, you can set them to the precise level of risk suitable to meet the business goals and objectives of your automotive eCommerce operation.

Kount fraud experts provide guidance and insight to each merchant, helping them get better at fraud mitigation. Kount's Rules Engine then makes it easy for merchants to fine-tune rules and thresholds so that detection and prevention responses are customized to each customer's specific appetite for risk. Our "how can we approve more good orders" approach lets online automotive retailers accept more orders from more people in more places than ever before.



5. Chargeback Alerts

When is a chargeback not a chargeback? If you intercept a transaction before the issuing bank applies it to your merchant account as a chargeback, you avoid chargeback fees. But how?

It typically takes 45 days from the time a chargeback is actually incurred until a merchant is notified. Yet card issuers often know within hours about a chargeback! It's the lengthy reporting process that introduces the 45-day "Chargeback Lag."

Fortunately, innovative, cooperative networks of merchants and card issuers—like the one founded by Ethoca—avoid this "Chargeback Lag." With Ethoca Alerts, card issuers send electronic alerts in as little as 1 hour so merchants can intercept bad orders before they become chargebacks. This helps merchants:

- Avoid merchandise and shipping losses, chargeback fees, etc.
- Identify other fraudulent transactions linked to the original bad order and halt them, too.
- Approve more borderline transactions (higher sales) yet still reduce chargeback rates.

Kount integrates Ethoca alerts and reporting to reduce admin time by as much as 75% and automate much of the process of linking other fraudulent transactions to bad orders.



6. Simple, Affordable SaaS

Easy, affordable, predictable. Software as a Service (SaaS) greatly simplifies fraud prevention and eliminates many costs.

Simple implementation, low-cost. Avoid expensive IT integration projects and eliminate the costs for technology, IT and headcount that are associated with in-house, “do-it-yourself” installations, as well as a number of third-party solutions.

Minimal rules. Seek out solutions that combine built-in fraud expertise, AI machine learning, and easy rule writing to deliver integrated, comprehensive fraud prevention that not only fights fraud, but boosts sales (fewer false positives) and lowers costs (fewer manual reviews).

Scalable. Easily handle seasonal surges as well as future growth.

Kount's SaaS solution features a simple implementation that's measured in days—not weeks or months—with no servers or storage arrays to buy. Built and supported by card-not-present fraud experts, it provides sophisticated, enterprise-class capabilities that are easy to use. Kount's “how can we approve more good orders” approach also delivers better returns than competing “how can we decline orders” approaches.



Avoid a Major Breakdown.

Before you get hit with big losses, higher expenses, and falling revenue, discover how a tune up of your fraud prevention capabilities can make your operations hum.

SCHEDULE A LIVE DEMO

“We really love the fact that Kount is a network. With capabilities like Order Velocity across a large number of retailers, fraudsters get identified in the Kount network right away.”

AWARD-WINNING RESULTS



Liz Lee
eCommerce Manager

