THE SECRET TO FRAUD PROTECTION:

Outsmart the bad guys

It's important to find a balance between protecting credit card information and delivering the best customer experience. In the recent Payments Primer: Tokenization we addressed the benefits of tokenization and online security.

When it comes to fraud protection, recent examples from large online retailers have shown that despite best efforts, major brands continue to suffer from credit card fraud.

Ecommerce fraud grew at an incredible 33%[1] from 2013 to 2014, underlining the increasing threat to merchants, their bottom line, and consumer confidence. In the U.S., the first steps have been taken to fight this trend with the mandatory EMV rollout in October of this year. The EMV rollout mandates that all cards issued in the United States must have "chip and signature" functionality. If you have been receiving new credit cards through the mail recently with shiny new chips in them, EMV is the reason why.

Problem solved? Not quite. EMV reduces the risk of point of sales (POS) fraud, but fraudsters will look for other ways to utilize their collection of stolen credit cards.

When similar laws were put into effect in Canada and the UK, POS fraud decreased but card-not-present (CNP) transactions grew. In effect, offline fraud went online.

But it's not all doom and gloom. According to a recent study by CyberSource[1], the "majority of merchants are experiencing lower rates of order rejection while keeping fraud losses stable." The good news is that fraud management works. The bad news is that the bad guys keep finding ways around even the most effective fraud management strategies. This means that merchants need to always be a step ahead of the bad guys.

The good news...

Adoption of EMV has had significant effects on fraud rates worldwide. Europe has seen an 80%[1] reduction in credit card fraud after adopting EMV. Canadian dollar losses due to card skimming have declined by nearly 40%[2] after EMV implementation. On the other hand, the US has seen a 47%[1] increase in credit card fraud, where EMV adoption is lagging.

Since hackers have a supply of fraudulent cards, they will use them on the path of least resistance. EMV constructs a barrier to use fraudulent cards for POS purchases. Therefore the path of least resistance will be online transactions

(1) Discover Financial Services, 2013
(2) Chase Paymentech Solutions, 2012

THE SECRET TO FRAUD PROTECTION:

Magento®

What's a merchant to do?

Balance is critical when developing a fraud prevention strategy. It is common to "fight fire with fire" – if your business is being attacked left and right, you want to control the problem immediately to protect your customers. Consider the impact of an onerous fraud management strategy on your customers? You don't want to make it hard for customers to do business with you, but you do want to keep them safe. There needs to be a balance between minimizing business risk and optimizing the customer experience.

The real issue with Fraud is that, on the whole, it represents a small amount of merchants' total transactions. With average fraud rates approximately 0.9%[1] of total transactions, finding the bad apples is like looking for a needle in a haystack. The key to making this more manageable is to change what merchants are looking for. Instead of looking for bad transactions, it's critical to identify good customers, and therefore good transactions. This way we can reduce the size of the haystack and more effectively fight fraud.

Good Customers should never know your fraud management strategy exists, except in rare instances where you have prevented fraud on their behalf and are calling to inform them and advise them what

action to take. The key is to identify good customers and frustrate criminals. Don't force your customers to take on the responsibility of your risk management. Know your customer's information, spending patterns and order history. Use this information together with past decisions to gain insight into current transactions. This helps you identify good customers so you can focus your fraud detection activities on a smaller set of transactions that may actually be fraudulent.

Fight back and make it difficult for the criminals to get what they want.

Fraud protection tools

So what tools counteract the evolving tactics of fraudsters? Braintree, a PayPal company, includes a version of Kount at no extra cost. Kount is a dedicated credit and debit card fraud detection solution that is helping merchants identify fraud more easily. In the past merchants have had to find trends or clues within their own data to identify fraudulent transactions. The "Kount Network" aggregates patterns and trends from across all Kount subscribers to help spot fraudsters. If a credit card has been found to be faulty in any of the 4 billion+ transactions they review globally, the transaction is flagged as "risky". Because criminals attempt to hide their true IP location from standard fraud tools, Kount combines both IP piercing and device fingerprinting technologies to accurately tie individuals to their purchases. If an IP is found to be coming from a strange location or a card is being used on far too many devices, Kount will flag transactions accordingly. All of this information is accumulated to generate a score for each transaction. This score helps merchants to identify 'good customers', giving them an undisturbed, seamless transaction experience on their site. The remaining 'flagged' transactions can then be reviewed manually OR through an automated set of rules that the Merchant identifies.

THE SECRET TO FRAUD PROTECTION:

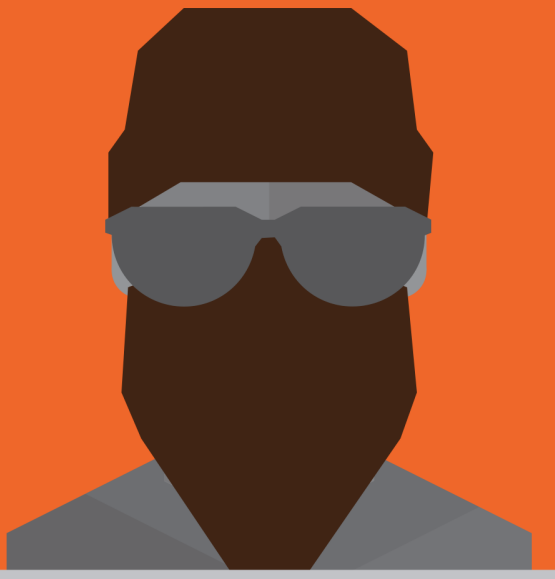
Magento®

HERE'S HOW THE DATA STACKS UP[3]

FRAUD RATE .9%

ORDERS MANUALLY REVIEWED 27%

2.3% ORDER REJECT RATE



85% ORDER ACCEPTED AFTER MANUAL REVIEW

10% FALSE POSITIVES

CHARGEBACKS 43% OF ALL FRAUD CLAIMS ARE CHARGEBACKS

The Online Fraud Management Benchmark Study published by CyberSource helps merchants gauge their performance against peer organizations by providing an overview of cross-industry performance, trends and challenges.

More About Braintree

Braintree, a PayPal company, helps online and mobile businesses around the world accept credit and debit card payments by providing a merchant account, payment gateway, recurring billing and sophisticated fraud management tools. The Braintree Payments extension connects your Braintree Gateway account with your Magento store, so customers can quickly and easily begin accepting credit card payments.

Increase conversions	*Reduce risk of fraud*	*Better service*
Tokenize credit card information in Braintree's PCI compliant vault, for a better, more secure checkout experience.	Braintree integrates industry leading fraud protection via Kount, the industry leader.	Manage customer exchanges and errors over the phone without requesting the credit card information a second time.

US SALES: +1.877.511.5036
US SUPPORT: +1.877.434.2894
HTTPS://MAGENTO.COM/PAYPAL/COMPLETE-PAYMENT-SOLUTIONS

Magento®

(3)Online Fraud Management Benchmark Study, CyberSource 2014-2015