



**Fighting Fraud: Finding the right
combination of solutions to stay one
step ahead**

**A Retail Decisions
Fraud Prevention Whitepaper**

2011 Edition

CONTENTS

| | |
|---|-----------|
| EXECUTIVE SUMMARY | 3 |
| HOW FRAUDSTERS ATTACK | 5 |
| UNDERSTANDING THE RISK OF SELLING GLOBALLY | 9 |
| HOW ReD PUTS IT ALL TOGETHER | 12 |
| ABOUT ReD | 14 |

Executive Summary

Thieves follow the money and there is a lot of it to be found in e-commerce. With consumers more comfortable than ever shopping online, e-retail sales are again enjoying exceptional growth. Worldwide e-retail sales are projected to grow at an annual rate of 19.4% and hit \$963 billion in annual dollar volume by 2013 states a report by investment bank Goldman Sachs entitled “Nothing But Net: 2011 Internet Investment Guide.”

Given the explosive growth in online sales it’s no wonder criminals are attempting more fraudulent transactions online than ever. Card not present fraud now accounts for more than 50% of all fraudulent transactions and that percentage is growing annually.

What’s more retailers are inadvertently opening the door to fraud wider by offering services that provide consumers instant gratification. Buying an item online and pick-up in-store programs promise fulfillment within 30 minutes or less.

The shortening window between when the order is placed and fulfillment is creating an immense need for retailers to screen transactions for fraud in real-time, rather than in batch at the end of the business day. Batch screening was only practical when items were shipped two business days or more after an order was placed. Recognizing this potential hole in the system, criminals are launching more attacks against retailers that offer shorter windows between processing an order and fulfillment so they can perpetrate fraud before the transaction is screened.

“Retailers are increasingly competing on logistics and that requires real-time, all the time fraud screening,” says Carl Clump, CEO of Retail Decisions Ltd., a world leader in card fraud prevention and payment processing. “Without real-time, all-the-time fraud screening merchants are more vulnerable to fraud, especially for transactions that cannot be thoroughly screened before the item is picked-up or shipped.”

What’s more, criminals are attempting to take advantage of retailers that expand their online

business globally. Entry into a new country poses many issues for retailers and fraud risk ranks high on the list. Doing business cross-border means accepting new payment options, many of which are local and each of which comes with its own risk sets. Further, consumer behavior varies by country. Behavior that may indicate fraud in one country may be perfectly legitimate in another.

Navigating these issues requires a fraud detection partner capable of measuring the risk for all payment preferences, from alternative payment options to general purpose credit cards. It also needs to be able to distinguish between legitimate and suspect consumer behavior patterns country-by-country, city-by-city and even neighborhood-by-neighborhood. With fraud rings' growing sophistication at hiding their tracks, this in-depth level of screening must take place in real-time to ensure that no transaction slips through the cracks.

“There can't be a generic, global template to fraud detection,” says Clump. “Fraud detection strategies have to be customized to each market, continually adjusted to keep pace with evolving fraud trends and enacted in real-time. It requires a lot of resources and for many retailers

the best solution is to partner with a fraud detection specialist that can provide the global perspective needed to detect fraud, prevent legitimate transactions from being rejected and can adjust its strategy globally as new fraud trends emerge in one part of the world before they spread to another.”

I. How Fraudsters Attack

Despite fraud losses from online transactions in North America still totaling less than 1% of online purchases, and online fraud losses in the United Kingdom dropping by 10% in 2010, maintaining a low ratio of fraud to overall online transaction volume is getting tougher. The growth in online transaction volume is emboldening criminals to attempt more fraudulent transactions. In the UK, for example, fraud attempts increased fourfold between 2009 and 2010, according to data compiled by Retail Decisions (ReD).

Fraud risk is also expected to increase as certain events that spur a lot of purchasing activity take place. For instance, fraudulent activity is projected to increase in the UK as the country prepares its run-up to the 2012 Summer Olympics. ReD detected a similar pattern in China as the start of the 2008 Summer Olympics neared.

“Fraud attempts will rise in regions criminals think are easier to attack or where fraudulent transactions are more likely to go unnoticed because of a sudden spike in transaction volume that can make it harder to

detect suspect transactions,” says Clump.

With criminals more organized, technically sophisticated and better financed than ever, real-time fraud detection is a necessity for any online merchant.

One such scheme is a bot attack. Internet bots, also known as web robots, are software applications that operate a bank of computers directed to complete specific tasks in a repetitive manner, but at a much higher rate than is humanly possible.

Criminals can use bots to direct large computer banks to initiate simultaneous fraud attacks on multiple merchants. The bot instructs each computer under its command to log onto a merchant’s web site and purchase a specific product. The strategy, often referred to as grab and dash, is twofold: first criminals want to hit a merchant as many times as possible before the scheme is detected and shut down. Second, bots allow criminals to spread their attacks across a broader merchant base to increase their success rate. Each computer utilized in the scheme can be programmed to move from one merchant to another on the target list so that fraud detection systems do not see the same computer accessing the

merchant's web site over and over in a short period of time, which is a major red flag.

During the 2010 holiday shopping season, ReD detected a bot attack being perpetrated against one its merchant clients. The bots had been programmed to target specific items, in this case electronic gift cards. The appeal of electronic gift cards to criminals is that they can be immediately downloaded from the merchant's web site and quickly resold for cash. The item is also popular with consumers, especially around the holidays, because they make great last minute gifts that can be emailed to friends and relatives.

Criminals tend to target top selling products that can be easily resold because these items generate not only high transaction volumes, but expected volume spikes around the holidays, both of which can make it harder to detect fraudulent transactions.

The incident in question resulted in a huge spike in transaction velocity for the merchant's electronic gift card that was uncharacteristic of normal velocity spikes, even for the holiday season. Thanks to its real-time fraud monitoring capabilities ReD was able to spot the anomaly and advise the

merchant to place a hold on fulfilling the suspect transactions.

In the meantime, ReD used its Red Shield® fraud detection service to pinpoint the transactions responsible for the spike in transaction velocity, determine characteristics common to each of the suspect transactions and reject them, all in real-time.

The retailer was spared a potential fraud loss of many thousands of dollars without denying legitimate purchases of virtual gift cards that were taking place at the same time.

Finally, ReD updated its database for its merchant clients around the globe so that transactions showing similar characteristics were immediately spotted regardless of the time of day the transaction took place.

"With digital goods, such as electronic gift cards, real-time fraud is about the only viable option for effective fraud detection before the item is downloaded," says Clump. "There is a high incident of fraud on digital goods because merchants have to make a decision on whether to allow the goods to be downloaded instantly. Real-time, all-the-time fraud monitoring creates a ring of protection that provides a major competitive advantage to all of ReD's merchant clients."

Other forms of bot attacks will target a group of products that are repeatedly purchased, such as an iPod, an iPod docking station and speakers. At first glance the purchase pattern may seem perfectly normal because it reflects a consumer buying accessories for a primary item. Only through in-depth, real-time analysis can a retailer determine if the pattern indicates fraud.

“Criminals may even change the product groupings, swapping out speakers for headphones and an in-car FM transmitter with an integrated iPod charger for the docking station, but there is always a pattern or common characteristic that indicates fraud,” says Clump. “That’s why neural technology is so important because it can analyze an infinite number of transactions, spot suspect patterns immediately and it constantly learns from the data it analyzes.”

Some of the fraud detection products by ReD include a sophisticated neural network technology called ReD Prism® which delivers a 10% lift in spotting fraud from traditional scoring models analytics and rules-based fraud monitoring applications. These tools make it possible for merchants to identify the

relationships among those components across multiple merchant categories and then assemble them in real time.

In addition, ReD hosts a suite of databases which contain the characteristics of more than 100 million fraudulent transactions from across the globe. These transactions are compared to an extensive database of known good transactions to spot variations that indicate suspicious activity.

Having accumulated such extensive fraud data, ReD can flag and review a suspect transaction as it enters the system and before making a decision whether to accept it, request more information from the consumer or reject the transaction outright.

Even if a merchant has the necessary resources to devote to fighting fraud, their ability to spot emerging fraud patterns is limited to the universe of their own transactions. ReD’s database of global fraud data is supported by teams of internationally-based seasoned fraud analysts that constantly monitor global fraud data to spot new trends as they move from one country to another, often in a matter of hours.

ReD Prism helps ReD's analysts understand the relationship between data sets around a transaction so that rules can be set that keep their rejection rates in line with, or lower than, their overall fraud rates, while ensuring that no good transactions are declined.

Use of proxy servers is another method criminals will use to perpetrate fraud. Criminals will obtain the addresses of known proxy servers and probe them to see if they can pierce the server's defenses to create the appearance they are logged onto the server when communicating with the retailer's web site. Proxy servers are an excellent way for criminals to hide the fact their Internet Protocol (IP) address originates from a country that is a known hot bed of fraud. By using a proxy server, criminals can hide their geographical location by leaving a convoluted trail of clues about how they came to the retailer's web site.

To beat the scheme ReD employs proxy piercing, a technique that examines the IP address of the shopper's computer to determine if a proxy server is being used and to determine the true geolocation of the shopper's IP address. Knowing the true location of the shopper's IP address can help retailers determine

if the shopper resides in a country or region where a high percentage of online fraud originates.

"Criminals are constantly finding new technologies that expose loopholes in the system and will always attack the weakest link in the chain," says Clump. "To fight back merchants need a fraud detection partner that constantly evolves its fraud prevention practices and solutions."

II. Understanding the Risk of Selling Globally

Many fraud scams have a local flavor pegged to consumer shopping habits, local payment options and retailer profiles. Online merchants also need to be aware of the countries in which they are doing business. Many countries and cities in Eastern Europe and Asia are home to highly organized, well capitalized fraud rings that bring their own unique twist to fraud schemes.

As online retailers enter new markets around the world they quickly learn of the need to expand the payment options they offer to fit the payment preferences of consumers in those countries. Without the right mix of payment options, online merchants can limit conversion rates by turning away consumers that don't have credit cards or that prefer not to pay with them.

Understanding the risk associated with all payment options, from alternative ones to general purpose credit cards, is critical as each new payment type comes with its own unique risk of acceptance. Debit cards, for example, are prone to account takeovers by criminals that gather the sensitive data needed to do so, such as user names, personal identification numbers (PIN), account numbers and passwords directly

from consumers through phishing attacks. Once armed with this information, criminals can successfully masquerade as the accountholder, making online purchases using the accountholder's PIN and other personal and account information.

Phishing is typically carried out by emails or instant messages that direct recipients to apparently trustworthy web sites, such as their bank, and ask them enter details about their account information to verify their identity. Criminals have also used phishing to target PayPal users to gather account data.

Still, credit cards remain the most common form of payment among consumers, which is why ReD tracks consumer behavior and fraud patterns across specific types of credit cards, such as rewards cards, prestige cards issued to the high spenders with the best credit scores and plain vanilla credit. Each card type is targeted to a specific consumer audience with its own set of behavior and risk characteristics.

Criminals will also frequent online chat rooms where they can meet sellers of CVV codes and expiration dates, the payment card data merchants rely on to confirm the person making the purchase is in

physical possession of the card. Criminals can also use online chat rooms to connect with sellers of stolen identities, PINs and payment card account information.

“ReD monitors these types of chat rooms to find out what criminals are up to and what type of information they are gathering to avoid detection,” says Clump. “We use the information we gather to create risk detection strategies by payment type and then customize that strategy to fit the profile of their customer base and risk tolerance.”

One problem merchants often overlook when expanding internationally is how their client base changes. Expatriates pose a particularly vexing problem for merchants as they typically have a credit card issued from a financial institution in their home country, a mailing address in another country and frequently travel around the globe. Traditionally merchants operating in one country set rules that reject a transaction if the credit card’s bank identification number, the customer’s mailing address and their IP address are from different countries.

This hard and fast rule cannot be readily applied by merchants selling internationally because of the

expatriate factor. ReD’s team of analysts work closely with each merchant client, evaluating their potential fraud exposure to create a fraud detection strategy customized to meet the merchant’s specific business requirements. Regular ongoing analysis and service reviews with the merchant client ensure the strategy, and the fraud detection model that drives it, remain optimal.

“Our analysts become an extension of the merchant’s business,” says Clump. “And they continue to work closely with the merchant day in and day out. That’s a very important part of the ring of protection that full-service, real-time, all-the-time fraud detection provides.”

ReD’s continual review of fraud trends makes it possible to write fraud strategies that are not only country specific, but specific to cities and even neighborhoods within an urban area. Certain zip codes, for example, may include known homes used by criminals as fronts to receive goods fraudulently purchased. The homes may be rented by the criminal or occupied by a member of the fraud ring in order to receive items that require a signature upon delivery.

“A lot of merchants are aware of the countries that are the hotbeds for fraud activity, but they don’t know the neighborhoods within a city that are the fraud hotspots or how rapidly those neighborhoods change,” adds Clump. “Effective fraud detection is employed at the deepest levels.”

Controlling fraud is not only the concern online merchants have as they expand globally; they must also manage credit card chargeback levels as they directly impact the interchange rates paid. A merchant with a high incident of chargebacks will pay some of the highest interchange rates.

Over the past year, incidents of so-called friendly fraud, where a consumer places an order and claims they never received the item have risen considerably. Contributing factors are the sluggish economy and consumers’ increasing knowledge of the chargeback dispute rules, which merchants must abide by if they accept general purpose credit cards. Anecdotal evidence suggests the economic conditions are prompting a growing number of consumers to dispute purchases as a way to compensate for lost income and still purchase some of the non-essential items they crave.

ReD works with its merchant clients to develop strategies that can curtail friendly fraud, such as device fingerprinting, a technique that captures a summary of software and hardware settings collected from a computer or mobile device used to access an online retailer’s web site. If the owner of the device contacts the merchant’s customer service department using the same device to dispute a transaction, the fingerprint can help the merchant counter claims the item was never received by proving the device was used to make a purchase.

Just as important is that device fingerprinting can identify web access devices associated with previous chargebacks. ReD will put rules in place to ensure such devices are flagged and the merchant takes extra steps to verify delivery of the order, such as requiring a signature upon delivery.

ReD’s fraud detection capabilities also make it possible to detect collusion between employees of delivery companies and fraud rings by tracking orders to specific geographic areas, such as a neighborhood block where consumers are claiming non-receipt of goods. “We’ve seen this trend in the UK and we expect to see it elsewhere,” says Clump.

III. How ReD Puts It All Together

To stay ahead of fraud trends retailers need a partner that can provide myriad, real-time fraud detection technologies and apply them to transactions that originate anywhere in the world.

As a specialist in fraud prevention, ReD provides merchants with the multi-pronged fraud detection strategy needed to stay one step ahead of fraudsters on a global basis. Unlike many other providers of fraud detection technologies—some of which offer fraud detection as a part of a larger menu of payments services—ReD is fully focused on fraud prevention and detection. ReD provides real-time, round-the-clock fraud detection 365 days a year.

Unlike other fraud detection providers that service merchants in a specific region of the world, such as North America, ReD pools data from its merchant clients around the globe. This global presence allows its analysts to spot fraud trends in real-time as they emerge in one country or time zone within a specific country and set rules—again in real time—to thwart the fraud threat

before it spreads to other countries or time zones.

ReD also recognizes that e-commerce is a round-the-clock business. Consumers will shop at any hour of the day depending on their work schedule or free time. Not having a fraud detection partner that is monitoring transactions between 12 am and 7 am because they are batch processing the day's receipts or performing scheduled maintenance on their database leaves a gaping hole in an online retailer's fraud defenses. After all, criminals know that online shoppers do not confine their purchases to normal business hours. Hence, transactions made outside of normal business hours are less likely to arouse suspicion than they were a few years ago when fewer online merchants were thinking about running a global business 24/7.

One feature unique to ReD is its Gibberish Filter, which detects brute force attacks using random keyboard strokes within an e-mail address or a physical address. This filter recently prevented 40 such attacks from one ReD merchant client in a single day.

Comprehensive detailed reporting is another feature that sets ReD apart

from the competition. ReD's Customer Service Interface (CSI) provides merchant clients with access to a web-browser facility that details all transactions received by ReD for fraud screening. With CSI merchants can securely view summary reports that include data on the number of transactions processed and the response that ReD provided, as well as search for and view specific transaction details, such as the outcome of each transaction within a given period.

Finally, merchants can search the CSI for transactions related to other transactions by any of the elements contained within the transaction, for example email address or IP address. "ReD provides a comprehensive, fully managed service for a single price," says Clump. "For online merchants, or any merchant, that is great value, because they don't have to pay for extras or worry about hidden fees to receive the full level of service promised."

With fraud detection playing a more strategic role in an online retailer's business and the cost of fraud detection accounting for a larger portion of their operating budget, having a partner like ReD can provide online retailers with the

competitive advantage needed to succeed globally.

About ReD

Retail Decisions (ReD) is a world leader in card fraud prevention and payment processing. A specialist supplier to the payments industry worldwide, ReD has over 21 years experience in the fraud prevention market. Its blue-chip international clients come from the global telecommunications, retail, travel, petroleum, banking and the broader e-commerce sectors. They include Air China, Coles, Comet, John Lewis, Singapore Airlines, Shell, Shoprite, Target, Tesco, Chevron, T-Mobile, Virgin Mobile and Walmart.

The company has offices in Australia, China, South Africa, United Kingdom and United States, with representation in India, Korea, Japan and South America.

Contact

USA

Kevin Sprake
Ksprake@red-usa.com
Tel: +1 732 452 2440

Europe and the rest of the World

Kami Boyer
Kboyer@redplc.com
Tel: +44 1483 728 700

www.redplc.com