Understanding and Combating Online Fraud in 2014

Fraud is pervasive online and high-risk merchants must be vigilant in employing a multi-layered, comprehensive approach to security and risk management. Merchants lost a staggering $3.5 billion in revenue to online fraud in 2012.[1] The anonymity afforded by the digital marketplace gives rise to daring fraudsters and increased loss for unprotected merchants.

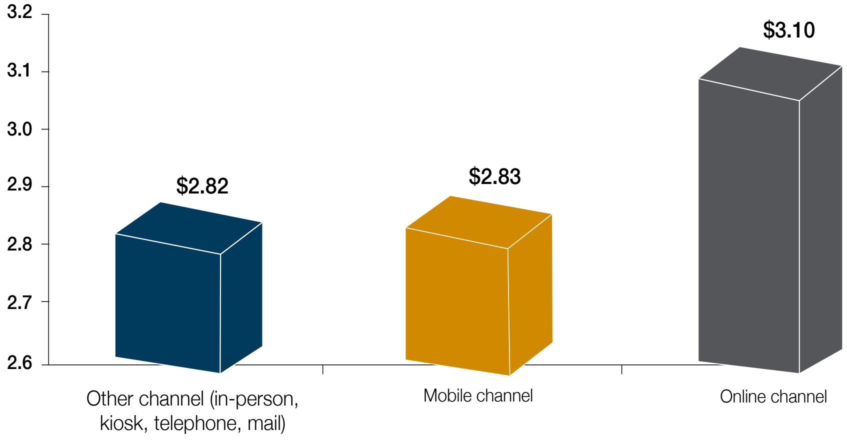
Merchants without a proactive fraud and risk management strategy are lagging behind these clever fraudsters and putting themselves at risk for loss of inventory, increased chargebacks and an unhealthy dent in their bottom line. Anyone that conducts Card Not Present ("CNP") business online, via the telephone or through mail is a target.

In looking at 2012 alone, the prevalence of online fraud is glaring:

- **61%** of organizations experienced attempted or actual payments fraud[2]
- **27%** of them report that the number of fraud incidents increased[3]
- The typical loss due to payments fraud was **$20,300**[4]

These upward trends in fraud have continued in 2013. According to the 2013 LexisNexis® True Cost of Fraud Study, there has been a spike in online fraud, costing merchants a hefty $3.10 for each dollar of fraud losses incurred. Fraud in the online channel is more costly than that encountered in-store or via mobile.

Figure 22. LexisNexis Fraud Multiplier Cost By Fraud Channel



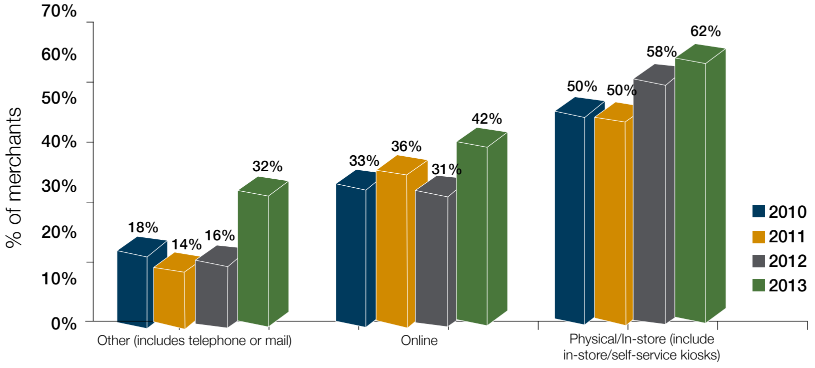
Weighted merchant data

Q: In thinking about total fraud losses suffered by your company, please indicate the distribution of various fraud costs over past 12 months.

May 2013, n varies 41 - 152
*Base = Merchants experiencing greater than $0 fraud through specific payment channels
©2013 Javelin Strategy & Research

The typical loss due to payments fraud was $20,300

Figure 8. Percent of Fraudulent Transactions Attributable to Channels Among Merchants Accepting Specific Channels



Weighted merchant data

Q: Thinking about the total fraud losses suffered by your company in the past 12 months, to the best of your knowledge, what is the percentage distribution of fraud over the following sales channels.

July 2010 - May 2013, n varies 58 - 176
*Base = Merchants experiencing fraud amount greater than $0 in the past year and accept payments through particular channels.
©2013 Javelin Strategy & Research

It has become significantly easier for fraudsters to get stolen card information and other sensitive data online and anonymity makes it incredibly easy to perpetrate fraud against CNP merchants. In fact, 42% of fraudulent online transactions can be attributed to these high-risk merchants. This is up from 31% in 2012.[5]

Understanding Risks with CNP Transactions

PCI DSS COMPLIANCE

The Payment Card Industry (PCI) Data Security Standard (DSS) framework was implemented to help guard against these types of breaches and strengthen security around merchants' cardholder data. PCI DSS compliance is a necessity for merchants, not only to security sensitive payment information, but also to gain and retain consumer confidence that their data is safe. While adherence to these principals is required, it is only the beginning of an effective fraud strategy.[6]

GOALS	PCI DSS Requirements - Validated by Self or Outside Assessment
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software
	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to cardholder data
	11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security

By implementing automated evaluations, merchants can protect themselves without breaking the bank

FRAUDSTERS ARE ADAPTING

Despite these security measures put in place, fraudsters have complex and sometimes not-so-complex tricks up their sleeves. There are a variety of tactics these cyber criminals utilize from highly complex techniques to simply buying stolen card information online. According to Rey Pasinli, executive director of Total Apps Inc., stolen credit-card accounts with full Address Verification System (AVS)-matched data are available for sale on the Internet for 8 cents per record.[7] With stolen payment data, cyber criminals or botnets controlled by fraudsters can have open season and thieve as much as possible. Other popular fraudulent activities include:

- Skimming
- Carding
- BIN Attacks
- Chargebacks

Mapping a Game Plan for Fraud Prevention

TWO-TIER PROTECTION MODEL

A fraud detection program should be robust. By implementing automated evaluations, merchants can protect themselves without breaking the bank. This should be supplemented by a manual investigation to cover off on any gaps and to add a deeper layer of review for any suspicious activity. The following safety measures should exist as part of the automated evaluation:

- Fraud-scoring models
- Address Verification Service (AVS)
- Device fingerprinting
- Card Verification Value 2 (CVV2)
- IP Geolocation

Any transaction that raises a red flag in the automated process should be handed off to a review team for further analysis.

Another key component of effective risk and fraud management is analysis for both process optimization and also for the development of key metrics. This type of analysis allows merchants to identify patterns in fraud and chargebacks and adjust processes accordingly. An added benefit is added efficiency and improved customer service.

FOLLOWING BEST PRACTICES

There are several steps a merchant can take to ensure they are protecting themselves to the highest degree. Outlined below are some of the security essentials that all merchants should adhere to in order to protect against fraudulent transactions:

CVV2 VERIFICATION – By requesting the three-digit code as part of the CNP process, merchants can be sure that the person placing the order has the card in his or her possession, adding another layer of security.

AVS AUTHENTICATION – Utilizing AVS allows merchants to verify the cardholder's billing address with the data on file with the issuing bank.

DIGITAL FINGERPRINTING - Digital fingerprinting allows analysis of a remote device and its characteristics, including installed plugins and software, time zone and other identifying features of the device. By identifying potentially fraudulent devices, merchants can take preventative measures.

IP GEOLOCATION - Sourcing geo-location and proxy-piercing information via IP address provides non-invasive insight into the risks involved with accepting transactions from specific IP addresses.

TELEPHONE VERIFICATION – Reverse phone lookups allow merchants to verify that the supplied telephone number matches address information and assess legitimacy.

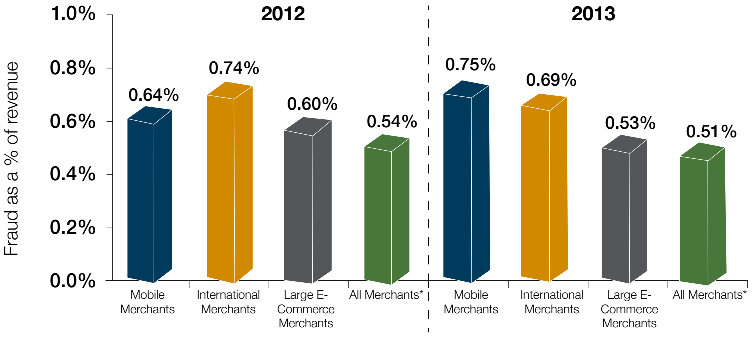
NEGATIVE LISTS – By leveraging customer history data, merchants can pinpoint "problem customers" and add them to a list. Merchants can then "red flag" future transactions by previous perpetrators and examine suspicious orders.[8]

RELATIONSHIPS WITH FINANCIAL INSTITUTIONS – Chargeback costs affect both merchants and FIs, regardless of liability. Cooperation and information sharing is an opportunity for both sides to benefit in that fraud attempts can be identified earlier, reducing loss and costs associated with chargebacks.

Employing a Vendor Can Be a Win

Large online merchants have experienced the greatest decrease in fraud compared to other merchant types. This is likely because – as the group that loses the greatest percentage of revenue to fraud[9] – they understand the importance of a holistic approach to fraud and risk management. In addition to decreased losses, they also recognize the benefits through increased sales and improved customer service. Fraud is not preventable, but these large, e-commerce merchants understand that ongoing investment in fraud prevention can yield dividends and improve bottom line.

Figure 4. Fraud as a Percent of Revenue by Merchant Type



*Weighted merchant data

Q: What is the approximate dollar value of your company's total fraud losses over the past 12 months? Fraud losses as a percent of total annual revenue.

July 2012, July 2013, n = varies 118 - 1,139
Base = All merchants, Large eCommerce Merchants, International Merchants, Mobile Merchants
©2013 Javelin Strategy & Research

MANY MERCHANTS LACK COMPLETE COVERAGE

While most merchants have some sort of fraud prevention or detection practice in place, they can be better served by augmenting with third-party fraud prevention services and tools. Not only does this ensure that a fraud prevention strategy is comprehensive, but it also allows merchants to focus on operations and their business while allowing specialists with expertise and ongoing insight in fraud prevention to handle the details.

While e-commerce sales continue to grow, eMarketer Inc. reports that less than a quarter of retailers are not keeping pace in terms of fraud protection, with less than a quarter expanding their risk management spending in 2012.[10] The types of tools that merchants employ vary, ranging from device fingerprinting, fraud-scoring models, IP geolocation and "Negative" lists, to name a few. Overall, merchants are implementing 4.9 fraud and risk management tools on average.[11] Some of the most popular risk management tools, in the order of effectiveness according to merchants perception from highest to lowest, include:

- Fraud-scoring model
- Multi-merchant purchase velocity
- Paid-for public records services
- Card verification number
- Order velocity monitoring
- Shared negative lists
- Social networking sites
- IP geolocation
- Device fingerprint results
- Customer order history
- Contact customer to verify order
- Payer authentication
- Address verification services
- Negative (in-house) lists of risky accounts
- Two-factor phone authentication
- Contact card issuer

Fraud scoring models are most popular with merchants, as they provide calculations to rate the risk level of each order based upon the order's value as well as factors attached to a credit card number, including past fraud.[12] While models like this can be beneficial, cherry-picking fraud prevention tools based on popularity is sure to leave gaping holes in an overall risk management strategy.

VERIFI'S COMPREHENSIVE FRAUD AND RISK MANAGEMENT SERVICES

Verifi's best-of-breed fraud and risk management solution can be tailored for large and small CNP merchants alike. The Intelligence Suite® offers a full-scale approach to combating fraud and securing customer data:

PROBLEM Anonymizing proxies allow fraudsters to use stolen or fraudulently obtained credit card data to make purchases (CNP and Click Fraud).

SOLUTION **IP Intelligence®**: IP address sourced geo-location and proxy-piercing information, provides in depth, non-invasive insight into the risks involved with accepting transactions from specific IP addresses.

PROBLEM Criminals have learned to thwart cookies and other inconsistent identifiers when making fraudulent purchases online, making unprotected CNP merchants an easy target.

SOLUTION **Device Intelligence™**: Device information and reputation scoring, deep packet inspection and additional proxy piercing capabilities expose the fingerprint and personality of the true device submitting the transaction.

PROBLEM Merchants are falling prey to increasing cases of friendly fraud where chargebacks are used as a form of shoplifting and customers claim they never received goods or services because of buyer's remorse.

SOLUTION **3-D Secure**: 3-D Secure or 3 Domain Secure is a cardholder authentication protocol for eCommerce transactions or card-not-present (CNP) purchases and covers 60% of US shoppers and 90% cardholders internationally and helps eliminate chargebacks. It helps prevent "I don't recognize" or I didn't do it" chargeback disputes from occurring.

PROBLEM Fraudsters are shrewd and shop for easy target CNP merchants to defraud before moving on to the next one, increasing chargebacks. It's almost impossible for any merchant to keep up on their own.

SOLUTION **Merchant Co-Op**: Merchant Co-Op is a powerful way for card-not-present (CNP) merchants to prevent chargebacks before they occur. New orders are compared against millions of orders taken by other Verifi merchants and scrubbed for possible fraudulent matches protecting against multiple types of fraud and risk. Merchant Co-Op is customizable to meet individual risk management thresholds.

High-risk merchants need to be aware of and proactive with the gamut of tools available in battling online fraud. While the obvious end goal is to defeat fraudsters and prevent the misuse of payment information, holistic fraud management also protects CNP revenue by instilling trust in merchants by consumers. Customer perception is everything when it comes to preserving volume. Almost one out of three identity fraud victims avoid specific merchants after being victimized.[13]

To maintain a competitive edge, CNP merchants will have to secure a solid front line defense against online fraud. An image of strong security will be paramount in assuring potential customers that their data is safe with a particular merchant.

About Verifi

Since 2005, Verifi has been a leading provider of global electronic payment and full-suite risk management solutions, helping card-not-present merchants improve their bottom line with industry-leading funds recovery rates of over 50%. The highly customizable payment and real-time reporting platform serves as a foundation for Verifi's suite of fraud solutions and risk management strategies. With a commitment of reducing risk while increasing profitability for clients, Verifi's multi-layered approach enables transaction risk management and mitigation, business optimization strategies, cardholder authentication and chargeback representment for all major credit card brands. Verifi is PCI Level 1 certified and headquartered in Los Angeles, California.

VERIFI™

For More Information

Main Phone: (323) 655-5789 Mon-Fri 8:00 AM – 5:00 PM PST
Main Fax: (323) 655-5537
Email Address: info@verifi.com

Mailing Address: 8391 Beverly Blvd., Box #310, Los Angeles, CA 90048

Citations

[1] http://www.internetretailer.com/2013/03/28/online-fraud-costs-e-retailers-35-billion-2012

[2] https://www.jpmorgan.com/cm/BlobServer/2013_AFP_Payments_Fraud_Survey.pdf?blobkey=id&blobwhere=1320596704807&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs

[3] https://www.jpmorgan.com/cm/BlobServer/2013_AFP_Payments_Fraud_Survey.pdf?blobkey=id&blobwhere=1320596704807&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs

[4] https://www.jpmorgan.com/cm/BlobServer/2013_AFP_Payments_Fraud_Survey.pdf?blobkey=id&blobwhere=1320596704807&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs

[5] http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf

[6] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[7] http://cardnotpresent.com/cnpexpo/h1.aspx

[8] http://usa.visa.com/download/merchants/global-visa-card-not-present-merchant-guide-to-greater-fraud-control.pdf

[9] http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf

[10] http://www.internetretailer.com/2013/03/28/online-fraud-costs-e-retailers-35-billion-2012

[11] http://www.internetretailer.com/2013/03/28/online-fraud-costs-e-retailers-35-billion-2012

[12] http://www.internetretailer.com/2013/03/28/online-fraud-costs-e-retailers-35-billion-2012

[13] http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf