



Do You Know Who You Are Doing Business With?

DIGITAL FINGERPRINTS AND THE EVOLUTION OF A COMPREHENSIVE FRAUD PREVENTION STRATEGY

Merchants must continually protect card-not-present (CNP) revenue from a variety of digital onslaughts, and more so than ever, be vigilant against online fraud. Identity fraud incidents affected 5.26% of adults in the country in 2012, driven largely by ballooning increases in new account fraud (NAF) and account takeover fraud (ATF).¹

More chilling is the fact that the online epidemic shows no sign of slowing:

- **61%** of organizations experienced attempted or actual payments fraud²
- **27%** of them report that the number of fraud incidents increased³
- **16%** report that the number had decreased⁴
- The typical loss due to payments fraud was **\$20,300**⁵


Speed Bumps in the Race to Slow Fraud

Despite advancements in online risk and fraud mitigation, merchants face several challenges:

“THE BALLOON EFFECT” – This describes the ability for fraudsters to effectively stay ahead of the fraud protection curve and circumvent the latest and greatest tools used by organizations. They do this by focusing on the most vulnerable and unprotected areas, though the more comprehensive a merchant’s fraud protection strategy, the more likely they are to be labeled a “hard target” by fraudsters and avoided.⁶

LACK OF RESOURCES – Risk management teams are expected to ensure optimal coverage at minimal cost. Unfortunately, slashing or stunting fraud protection budgets often means sacrificing the full coverage needed to sufficiently keep pace with evolving risks.

FLAT PREVENTION STRATEGY – Fraud prevention tools should be current, efficient, dynamic and multi-layered to be effective. Internal tools that work to uncover suspicious activity such as unmatched billing and shipping addresses or rapid activity tied to a specific IP or address can be useful, but not as useful as tools that have the capacity to analyze across an entire industry or network.⁷



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

INCOMPLETE SOLUTIONS – CNP Merchants should be using a combination of tools and services to achieve optimal fraud coverage in conjunction with their own data. While PCI DSS measures help protect against fraud in all channels (online, mail order and telephone orders), there are channel-specific tools that are necessary for complete protection.

CVV2 verification can be utilized for online and telephone orders. Address Verification System (AVS) security can be used for online, mail and telephone orders. 3D Security protects online orders. Merchants should, at the very least, be employing all of these measures where possible.

How does Digital Fingerprinting Help?

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. Much like an actual fingerprint, these identifiers create a unique signature. According to the Electronic Frontier Foundation, 94% of browsers using Flash or Java had unique identities.⁸

By implementing this type of fingerprinting, organizations can statistically identify devices based on a variety of indicators, including something as simple as identifying a difference between the clock on a user's machine and that on a website's server. Once potentially fraudulent devices are identified, a database of "flagged" threats can be created. The difference between digital fingerprinting and cookies is that the former looks at information websites already collect, whereas the latter involves storing unique identifiers on a machine. Data from eMarketer Inc. shows that device fingerprinting is one of the most popular fraud management methods to merchants, with 50% citing the tool as the most effective they use.⁹ According to Andras Cser, principal analyst for security and risk management at Forrester Research Inc., a company can see a 25%-35% reduction in fraud losses upon implementation of device fingerprinting.¹⁰



Why is Digital Fingerprinting Necessary?

Cyber criminals are becoming increasingly shrewd and turning to increasingly complex tactics to conduct their crimes online. The added benefit of remaining anonymous makes tracking and preventing these criminals difficult. The ability to thwart cookies is



Roughly \$36 billion of a total \$2.1 trillion in payments were made with a mobile device in 2013

old hat, so companies must turn to additional identifiers to protect themselves.¹¹ Small retailers must be extra vigilant as they experience the most dramatic impacts. Studies estimate about 15% of all fraud victims avoid small online merchants after an incident of fraud. This is a much greater percentage than larger retailers experience.¹²

An additional consideration is the future of mobile payments and subsequent implications for fraud prevention. People are increasingly paying bills via mobile and Javelin estimates that roughly \$36 billion of a total \$2.1 trillion in payments were made with a mobile device in 2013 for just seven common types of bills.¹³ With mobile payments set to reach \$633 billion in 2014 and mobile payment users growing to 490 million in 2014 from 81.3 million in 2013¹⁴, fraud prevention strategy will have to maintain pace. In 2012, mobile commerce operators lost 1.4% of revenue to fraud, or about \$300 million to \$400 million annually, according to Forrester Research Inc.'s estimate.¹⁵

Taking the next steps - choosing a vendor

While online fraud will never be completely eradicated, there are tactics that have been developed to help identify and combat illicit online activities. Digital fingerprinting, the method of collecting information on and identifying remote computing devices, has changed the online landscape. Digital fingerprints partially or wholly identify users and devices, including identifying if a device has cookies disabled.¹⁶

Additionally, some credit card providers like Visa have allowed for the use of particular digital fingerprints, such as purchaser's IP address and download time, to qualify as compelling evidence against certain reason codes for chargebacks.¹⁷ These additional representment rights pave the way for merchants to more aggressively fight chargebacks, though they can require significant time and in-house resources.

Staying abreast of the newest online threats can be a daunting task for merchants. Researching and implementing the correct tools and preventative strategies requires significant resources and costs can be high. Additionally, the wealth of information and data available can be hard to digest for merchants acting alone. Many merchants opt to employ a vendor that has the capacity to make sense of big data and identify patterns and create and manage a tailored, comprehensive fraud and risk prevention strategy based on this information.

Verifi's Intelligence Suite offers best-of-breed risk management and fraud protection for merchants looking to protect CNP revenue without sacrificing customer experience. Partnerships with leading-edge experts in IP address data, device information and reputation scoring and consumer information allow Verifi to provide unmatched protection and flexibility with one source integration. The comprehensive combination of solutions – which can be turned on or off at any time – include:

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.

The Intelligence Suite offers flexibility for merchants to choose which technologies are appropriate for their business and the ability to apply these technologies specifically to the transactions that require them. Through one-time integration, merchants can apply these solutions in real-time through Verifi's dynamic rules engine and to both financial and non-financial transactions.

Online fraud is not going away but its impact can be lessened for big and small merchants alike who opt for full-service risk management.

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 chargeback 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.



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 <https://www.javelinstrategy.com/brochure/276>
- 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 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
- ⁶ http://www.equifax.com/pdfs/corp/EFX-USA-2048_Suspicious_ID__WP.pdf
- ⁷ http://www.equifax.com/pdfs/corp/EFX-USA-2048_Suspicious_ID__WP.pdf
- ⁸ <http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/>
- ⁹ <http://www.internetretailer.com/2013/03/28/online-fraud-costs-e-retailers-35-billion-2012>
- ¹⁰ <http://www.internetretailer.com/2013/09/12/bh-photo-sharpens-its-focus-blocking-online-fraud>
- ¹¹ http://blogs.wsj.com/digits/2010/12/01/evercookies-and-fingerprinting-finding-fraudsters-tracking-consumers/?mod=rss_WSJBlog&mod=
- ¹² <https://www.javelinstrategy.com/brochure/276>
- ¹³ <https://www.javelinstrategy.com/brochure/299>
- ¹⁴ <http://gigaom.com/2010/05/13/mobile-payments-to-reach-633b-by-2014/>
- ¹⁵ <http://www.internetretailer.com/2013/05/01/securing-m-commerce>
- ¹⁶ http://en.wikipedia.org/wiki/Device_fingerprint
- ¹⁷ <http://usa.visa.com/download/merchants/compelling-evidence-dispute-resolution.pdf>