Just Right

3 PRIMARY THINGS MERCHANTS CAN LEARN ABOUT FRAUD PREVENTION FROM GOLDILOCKS

150,000 strains of malware are introduced every month.[1] According to The Aite Group, "in 2013 the number of breached merchant locations exceeded the 2012 total by mid-year."[2] This creates a unique challenge for merchants – how do you maintain a flexible and responsible fraud prevention strategy when integrations are often static and criminals are dynamic and constantly evolving?

As the tale of "Goldilocks" portrayed, merchants should create agile strategies to determine the amount of fraud risk that is "just right" for their organization without dramatically impacting legitimate sales.

Don't Be "Too Cold or "Too Hot"

Obviously, not enough fraud prevention is a mistake as merchants on average lost nearly 1% of total online revenue to fraud in 2012.[3] Also, as a result of the highly publicized data breaches and new fraud data, consumers are voicing a very real concern to a merchants' ability to prevent these adverse situations from occurring; merchants who ignore these concerns run the risk of damage to their brand and future sales.

On the flip side, overly sensitive fraud prevention hurts too – creating false positives, placing an undue burden on the manual review process and creating unnecessary friction in the checkout process. There can be as many as 40 false positives for every legitimate attempt at fraud (a 40:1 ratio), meaning that up to 97% of transactions flagged as high-risk can be legitimate.[4]

Simple economics or resource limitations sometimes prevent merchants from experimenting with new fraud tools and doing the fine-tuning necessary to be effective because an unfortunate and often overlooked fact is that integrating new tools can be terribly expensive and time consuming.

There is no such thing as "perfect" fraud prevention but by using the proper combination and balance of solutions, it becomes possible for merchants to quickly layer and then mix and match various fraud prevention tools to find the overall strategy that yields the best results.

Fraud is Here to Stay and Will Rise Naturally As Ecommerce Sales Continue to Expand

A stunning 61% of organizations experienced attempted or actual payments fraud in 2012, according to JPMorgan's 2013 study, with 27% of them reporting that the number of fraud incidents increased.[5] CNP Fraud will rise naturally and also be impacted by industry related actions:

It's estimated that Card Not Present ("CNP") fraud makes up about 1 percent of ecommerce revenue.[6] It is predicted that U.S. consumers will spend upwards of $430 billion on ecommerce transactions by 2017[7] with no sign of slowing.

ECOMMERCE SALES GROWTH THROUGH 2016

	2014	2015	2016
Forrester Research	$291 Billion	$319 Billion	$345 Billion
JPM Securities	$295 Billion	$331 Billion	$364 Billion
eMarketer	$297 Billion	$339 Billion	$385 Billion
Robert W. Baird	$272 Billion	$299 Billion	$329 Billion
Cantor Fitzgerald	$276 Billion	$304 Billion	$329 Billion

Source: eMarketer, April 2013, Figure 154501[8]

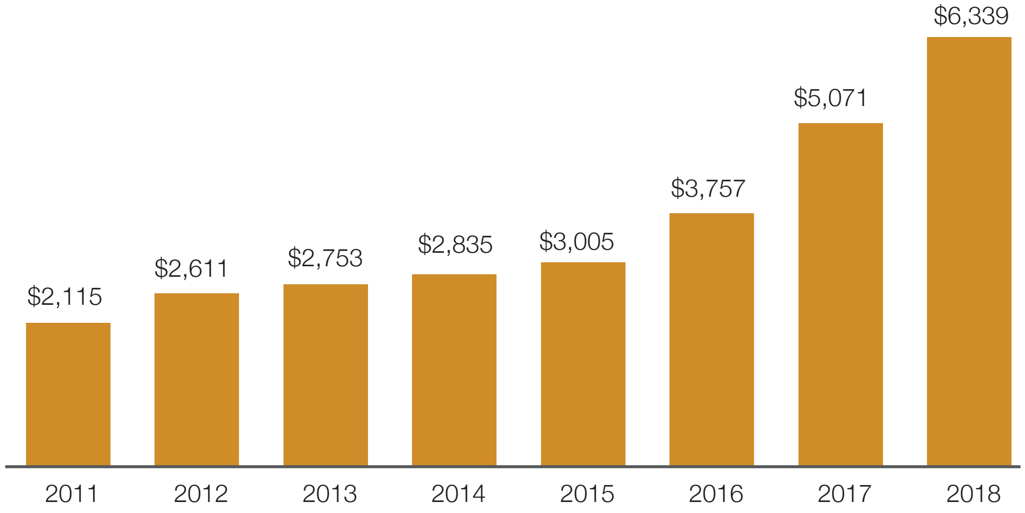
As ecommerce gains momentum, so will fraud. Last year, merchants learned the hard-way that fraud is here to stay. Retail mega-breaches compromised millions of payment cards and the HeartBleed Virus exposed a number of online data vulnerabilities. The curtailing of personally identifiable information (PII) also makes it hard to identify the fraudsters. PII available for verification and authentication purposes as publicly available information is on the decline. In 2013, only 30% of that information was publicly available compared to 78% in 2000. This is partially due to the increasing number of threats to PII and the response by websites and lawmakers to limit the accessibility and distribution of PII.[9]

In Market Events and Conditions Will Compound The Problem

Also, new concerns loom large as the implementation of EMV in the US begins next year. European rollouts of EMV showed significant increases in fraud as fraudsters move to CNP channels as a means of last resort, since card present fraud will virtually be eliminated. As illustrated in the chart below, CNP fraud is expected to more than double, after the implementation of EMV in the US marketplace.

Projected CNP Fraud Losses

U.S. CNP Credit Card Fraud Losses, 2011 to e2018
(In US$ billions)



Source: Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014

FICO published a number of predictions for the top fraud threats of 2014. Some of the biggest trends include:

- Unprotected mobile devices leaving consumers exposed to fraud
- Spoofing of smartphone apps luring unsuspecting consumers into downloading rogue versions
- As mentioned above, increased CNP fraud as the adoption of chip and PIN (EMV) technology takes hold in the US.[10]

Consumers Will Vote With Their Pocket Books

The threat of online fraud continues to be of great concern to consumers, with a recent Associated Press poll showing 58 percent have “deep concerns” about their personal data in online transactions.[11] Merchants that ignore this important consumer sentiment do so at their own peril, The impacts to their brand and future sales can hang in the balance; the 2013 LexisNexis® True Cost of Fraud Study points out that 29% of fraud victims avoid certain merchants as a result of their victimization, which can have a devastating effect on profits.[12]

While it’s evident that thin fraud protection is not advised given the trends and customer marketplace, merchants should be mindful of the possibility of going overboard and driving good customers away. While prudent fraud prevention ensures that bad and unlawful transactions are blocked (in most cases), it also has its limitations that create friction that turns away legitimate sales and customers as well.

THE PROBLEM: An Adaptable Fraud Prevention Platform is Necessary but Hard To Implement and Maintain

Finding that "just right" balance takes time and requires the full-view of the fraud management process and solutions across the entire operation, including: screening tools, risk models and rules, manual review process, order dispositioning and chargeback management. Establishing a baseline for these operations allows businesses to analyze and fine tune faster and more efficiently.

By continuously monitoring and adjusting indicators and patterns, and altering the weight of significance of each of these elements in accepting or denying a transaction, fraud models and rules controls give merchants significant power to not only prevent fraud but ensure that they are not turning away good sales by creating friction in the check-out process.

One size really does not fit all; each merchant should utilize a solution that allows maximum flexibility and customization that protects and streamlines the payment process, instilling confidence in customers without hindering the transaction flow.

There are countless fraud prevention tools available to merchants and this presents a major operational dilemma: implementing multiple tools often requires multiple vendors, multiple contracts and multiple integrations, which is expensive, time-consuming and difficult to fine-tune rapidly.

GOLDILOCKS LESSON #1: Use the Right Tools For Your Business

While there are numerous, best in class fraud prevention tools available, using the right one or combination of solutions for your business is a critical first step in setting up your fraud prevention solution for success and with the least impact to legitimate sales. You would not use a screwdriver to hammer in a nail. So using the proper tools applies to your fraud prevention tools as well to address your specific fraud vulnerabilities, while protecting against others. Here is a look at different solutions related to common types of fraud problems.

PAIN POINT	TOOL	CAUTIONS	"JUST RIGHT"
Fraudsters masked by anonymizing proxies use stolen payment card data to make purchases or commit click fraud.	**Digital fingerprinting:** 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.	• False positives and lost sales can result from reliance on this tool alone, without other validation tools. • Underusing this tool can result in higher-than-average instances of fraud that could be prevented	Fine-tuning this feature allows merchants to intelligently block transactions from fraudulent IP addresses.
Digital fingerprinting technologies are stunted by criminals that have learned to thwart cookies and other inconsistent identifiers when making fraudulent purchases online.	**Device Fingerprinting:** 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.	• Setting scoring levels too high can result in false positives, resulting in lost sales	Balancing Device Intelligence with IP Intelligence can strengthen controls without allowing one factor to override legitimate sales.
Criminals leverage affiliate networks to commit fraud through seemingly legitimate marketing channels, making it very difficult to detect.	**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 merchants and scrubbed for possible fraudulent matches protecting against multiple types of fraud and risk. Merchant Co-Ops can be customizable to meet individual risk management thresholds.	• Ultra-high risk thresholds put merchants at risk of turning away purchases made by valid payment cards	Using merchant co-op as a "booster" to IP Intelligence, Device Intelligence and 3-D Secure enables merchants to seal their risk prevention strategy by taking advantage of shared intelligence with other merchants.

PAIN POINT	TOOL	CAUTIONS	"JUST RIGHT"
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.	**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.	• Over-reliance on this tool alone does not provide adequate coverage as banks choose the mechanism they deem appropriate in verifying the authenticity of the purchaser, which may not always be foolproof.[13]	3-D Secure is a solid, fundamental security feature that can be fortified with other intelligence measures that have been tested and toggled to meet a merchant's specific risk threshold.
Lack of communication between card issuers and merchants means transactions suspected as fraud and cardholder initiated disputes snowball into chargebacks rather than potentially being avoided through issuer/merchant cooperation in addressing the issue, processing a refund or issuing a credit, ultimately preventing the chargeback.	**Post Billing Chargeback Alerts:** Immediate notification of cardholder disputes from the card Issuers helps stop the fraudulent shipments of orders before they become a loss and gives the merchant an opportunity to respond to the dispute and resolve the issue before it becomes a chargeback.	• Merchants should not rely on issuer alerts alone as front-end fraud prevention tools are necessary to maintain an acceptable chargeback ratio.	Augmenting fraud prevention tools with pre-chargeback notifications allows merchants to dial back front-end fraud prevention tools, decreasing false positives while respecting the limits of the risk threshold.
Fraudsters are able to use stolen card information to make online purchases where only card information is required for authentication.	**Facial Recognition:** This technology uses the location/ distance and ratios of features, such as eyes and ears, on a photograph to compare to reference data in order to confirm a person's identity.[14]	• May require use of specialized camera installation on devices; may require users to pay additional fees and may raise some privacy concerns over the storage of facial images in databases.[15]	When used in conjunction with authorization protocol and other fraud prevention tools such as 3D Secure and device fingerprinting, facial recognition can add a layer of protection and verification.
Fraudsters are able to use stolen card information to make online purchases where only card information is required for authentication.	**Voice Verification:** Voice recognition technology is a non-intrusive way to match a person's voice with their pre-recorded template to verify their identity.	• Health and emotional state can cause variance in a person's speech, causing a mismatch between voice template and sample submitted for verification.[16]	When used in conjunction with authorization protocol and other fraud prevention tools such as 3D Secure and digital fingerprinting, facial recognition can add a layer of protection and verification.

There are a lot of good tools at merchants' disposal so choose wisely and customize your strategy to employ the **right tools** at the **right level** for the **right situation**.

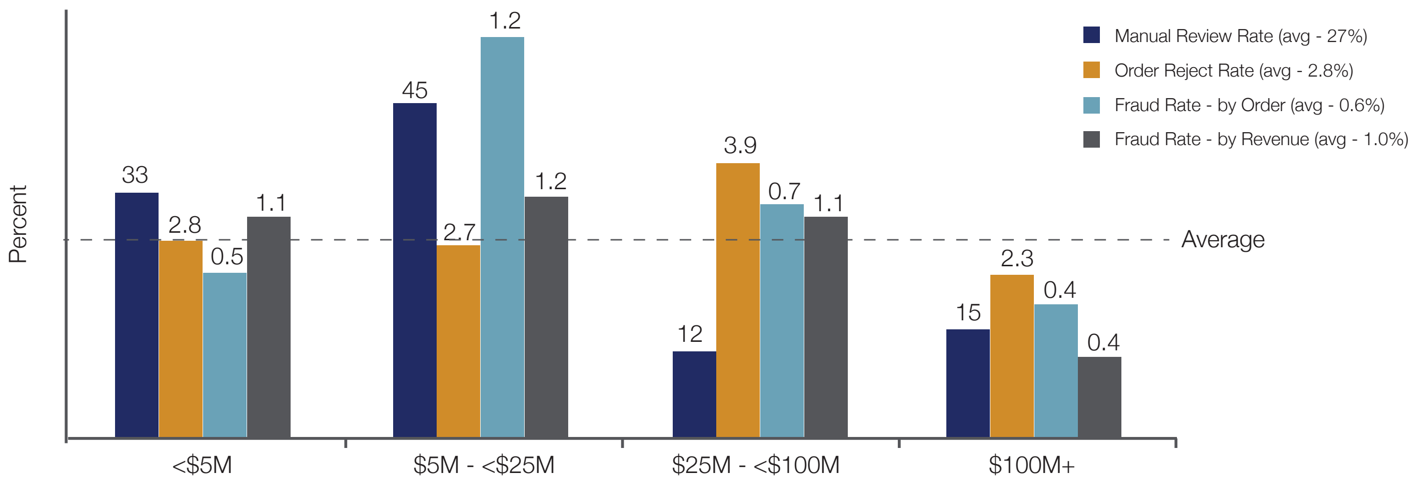
GOLDILOCKS LESSON #2: Utilize End-to-End Transaction Data to Identify Emerging Threats and Quickly Adjust Your Fraud Prevention Platform

Effective fraud prevention requires a solid, sensible combination of the tools mentioned in the previous section. Employing these tools in conjunction with analytics on high-risk transactions and supported by back-end feedback loops allows for a high level of accuracy without sacrificing legitimate sales.

When fraud prevention tools are combined with pre-chargeback notifications on the back-end, merchants gain a unified view into the entire transaction lifecycle.

A pre sale and post sale view alerts merchants of likely fraud incidents before they occur, allowing merchants to prevent the chargeback and address the issue. Companies must constantly weigh the tradeoffs between fraud loss, customer experience, and cost, in fine-tuning their operations to protect against the latest fraud attacks. Having baselines to measure against and a framework by which to address these tradeoffs can streamline the fraud management process.

Order Reject Rate and Fraud Rates by Merchant Size



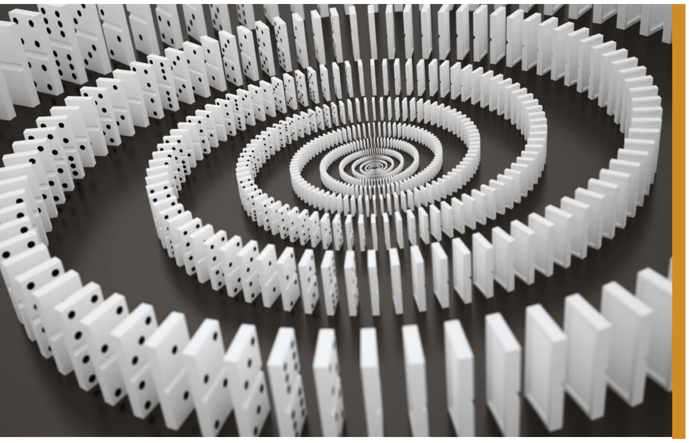
Tradeoffs exist between fraud losses (both fraud rates and revenue lost from good sales that were rejected), customer experience and cost. Fraud prevention is a balancing act that must constantly be fine-tuned.[17]

Businesses can execute more efficient and effective order screening by using an automated system to handle a majority of the decisions and using a review team only for investigation of the most suspicious orders. Manual review of orders to research and accept or reject suspicious orders can range from 4 to 15 minutes per order.[18] Since review teams are usually the largest cost in a business' fraud management budget[19], automating the majority of decisions and streamlining the manual review process can have substantial cost-savings implications.

THE IMPORTANCE OF FEEDBACK LOOPS ON THE BACKEND

Chargebacks can actually boost your fraud prevention awareness by acting as a feedback loop to front-end fraud prevention measures. By analyzing your fraud prevention strategy within the context of your operational goals and how you are meeting the business' overall financial objectives, you can better balance effectiveness and efficiency.

Keep the following key performance indicators (KPIs) in mind as you fine-tune your fraud prevention approach:



- Total chargebacks as a percentage of the number of orders
- Total chargebacks as a percentage of total transaction revenue
- Order dispositioning review times
- Amount of transactions reviewed
- Amount of false positives

Look at these KPIs within specific windows of time to establish good and bad trends and determine where improvement is needed. Merchants should use historical data to set a baseline for comparison moving forward.

At the end of the day, merchants must be mindful of the business impacts that fraud prevention solutions have on their business. When merchants *react* to fraud predictions rather than proactively taking into account the unique and particular risk needs of their business, they often end up with a fraud strategy that far overreaches what they really need. Implementing an agile fraud prevention solution means it will be continually refined over months and years. Once baselines are established, fine-tuning will be a constant and merchants should be able to easily merge new technologies with existing ones to augment and tailor on the fly. Unfortunately, as we will discuss, automating and fine-tuning those processes to guard against quickly emerging new threats is expensive, time-consuming, and a difficult feat to pull off alone.

GOLDILOCKS LESSON #3: THE NEED FOR SPEED – Adapt Quickly and Cost-Effectively to Positively Impact ROI

According to The Aite Group, there were approximately 58.4 million unique new strains of malware deployed in 2013 and that yearly production total will grow to nearly 166 million by 2017.[20] It is imperative that the fraud management strategy remains agile, which can be a tall order when you consider that fraud solutions take weeks or months to integrate or adjust and remain largely static after integration. This puts merchants at a huge disadvantage as it limits the ability to adjust fraud-scoring models on the fly based on back-end analytics and feedback loops.

Maintaining pace with rapidly evolving fraud can be difficult – merchants that accept online payments said 42% of fraudulent transactions came from the online channel in 2013, compared to 31% in 2012.[21] As such, merchants must find ways to speed up the implementation or adjustment of new fraud rules and other operational changes necessary to improve mitigation.

Integration traps hinder agile fine-tuning and are expensive

One of the biggest pitfalls for merchants is not utilizing real-time analytics to adjust and toggle their fraud prevention tools. This may be due to an inability to fully integrate because of time, resource or IT constraints. As mentioned, fraudsters are dynamic and threats are constantly evolving. Consequently, merchants and their solutions need to remain on pace to be adequately protected.

Merchants should utilize both predictive analytics and a rules engine that enables merchants to change and configure fraud tools on-the-fly, without having to disrupt their workflow with new integrations.

There is no getting around the fact that integrations are costly in terms of both real dollars or the time and resources needed to support them internally. Integrations can range from $0 – where the client is expected to do the entire integration set-up with no professional services or support – to ten of thousands of dollars or more. Additionally, this does not necessarily come with all the bells and whistles; rules strategy development, rules implementation, testing, training, support for life of the account, and quarterly releases of the solution may add additional expenses over time.

Each merchant will have to make it's own business case for various fraud prevention tools. Merchants who employ in-house solutions have to consider software development cycles and those who outsource have to consider integration cost and timeframe.

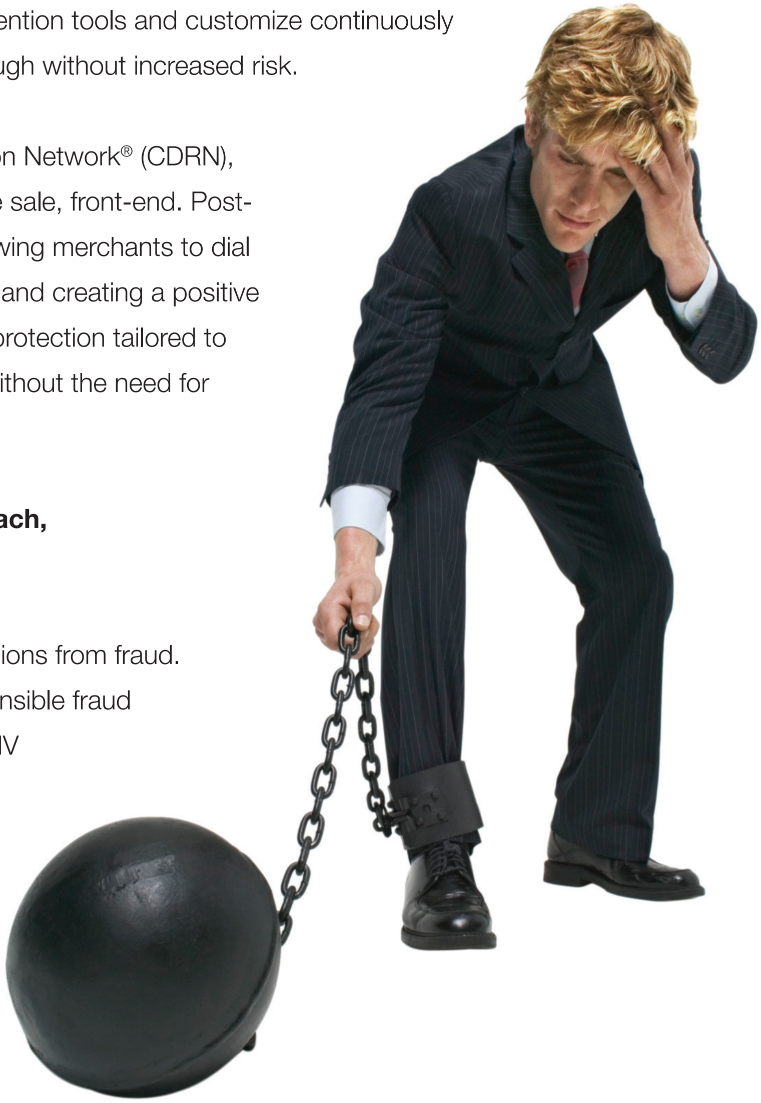
Consider outside expertise

When looking at the cost, time-commitment, number of necessary tools and rapid adaptation needed, merchants can look to employ outside help in achieving the right balance of fraud prevention and being able to effect modification more easily.

Verifi recognized how difficult finding that "just right" balance was for merchants and created its comprehensive fraud management platform, Intelligence Suite®, to allow merchants to layer and tailor fraud prevention simply and cost-effectively.

Rather than dealing with individual fraud solutions on a "one off" basis, Intelligence Suite provides a personalized technology hub that allows for the rapid integration and fine-tuning of fraud controls. Covering all the critical fraud prevention verification points, (such as consumer, device, mobile, IP geo location, and payments channels) the platform delivers top-of-the-line fraud prevention tools through one integration that can be modified easily with Verifi's proprietary rules engine. Merchants obtain the ability to test and toggle various fraud prevention tools and customize continuously based on results and to allow more successful sales to pass through without increased risk.

By combining Verifi's award winning Cardholder Dispute Resolution Network® (CDRN), merchants can minimize fraud loss without losing sales on the pre sale, front-end. Post-Billing Chargeback Alerts can reduce chargeback rates while allowing merchants to dial down upfront fraud screening, subsequently boosting conversion and creating a positive impact on the bottom line. This combination offers tightly woven protection tailored to meet a merchant's custom needs and address common issues without the need for multiple, costly and time-consuming integrations.



Fraud Protection that is "Just Right" – Use a layered approach, listen to all your data points and MOVE QUICKLY

There is no one "silver bullet" to protect card-not-present transactions from fraud. The goal for merchants should be to maintain a flexible and responsible fraud prevention strategy. As e-commerce continues to expand and EMV takes hold in the US, merchants will see fraud rise. Employing an adaptable fraud prevention strategy that is able to maintain pace with dynamic criminals and evolving threats in paramount.

Shrewd criminals are always innovating, creating new threats by the minute. Unfortunately for merchants, many of the platforms available to fight fraud require static integrations that are slow and costly, putting their transactions and their revenue at risk. To stay ahead of these fraudsters, merchants need to leverage proven technologies and tools, evaluate and analyze the type of fraud they are experiencing, and adjust fraud prevention tools quickly.

Every business is unique and "too hot" and "too cold" indicators will differ from merchant to merchant. By listening to Goldilocks, layering fraud prevention tools and toggling to find what is "just right" for your business, you can improve your risk prevention effectively and without breaking the bank on costly IT integrations and maintenance .

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 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.bankinfosecurity.com/julie-a-6119/op-1

2 20131008-Cyberthreats-MultiplyingLikeTribbles-Report-pdf_3765_18213_10125_7966.pdf

3 http://images.demand.cybersource.com/Web/CyberSource/CyberSource_2013_Online_Fraud_Report.pdf?utm_campaign=Fraud%20Report%202013%20-%20Form%20auto-reply&utm_medium=email&utm_source=Eloqua

4 http://blog.finsphere.com/2013/04/19/five-words-nobody-likes-to-hear-your-credit-card-was-declined/

5 Association for Financial Professionals; “2013 AFP Payments Fraud and Control Survey”; jpmorgan.com; March 2013; http://www.larutech.com/jan2014/2013_AFP_Payments_Fraud_Survey.pdf

6 “Card-Not-Present Fraud: A Primer on Trends and Authentication Processes,” Smart Card Alliance Payments Council, February 2014

7 “Card-Not-Present Fraud: A Primer on Trends and Authentication Processes,” Smart Card Alliance Payments Council, February 2014

8 http://www.emv-connection.com/wp-content/uploads/2014/01/CNP-WP-012414.pdf

9 Marketing Takeaways from AdExchanger Industry Preview 2014”; aggregateknowledge.com; January 2014; https://www.aggregateknowledge.com/2014/01/marketing-takeaways-from-adexchanger-industry-preview-2014/

10 http://www.biia.com/fraud-predictions-for-2014-beware-of-card-not-present-transactions

11 http://cardnotpresent.com/news/cnp-news-jan14/Report__U_S__Consumers_%E2%80%98Concerned%E2%80%99_about_Breaches,_But_Not_Showing_It_-_Jan__30,_2014/

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

13 https://blogs.cisco.com/security/the_3d_secure_protocol_implementation_flaws_and_possible_resolutions/

14 http://www.parl.gc.ca/content/lop/researchpublications/06-30-e.htm

15 http://www.parl.gc.ca/content/lop/researchpublications/06-30-e.htm

16 http://www.globalsecurity.org/security/systems/biometrics-voice.htm

17 https://www.jpmorgan.com/cm/BlobServer/13th_Annual_2012_Online_Fraud_Report.pdf?blobkey=id&blobwhere=1320571432216&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs

18 http://images.demand.cybersource.com/Web/CyberSource/CyberSource_2013_Online_Fraud_Report.pdf?utm_campaign=Fraud%20Report%202013%20-%20Form%20auto-reply&utm_medium=email&utm_source=Eloqua

19 http://images.demand.cybersource.com/Web/CyberSource/CyberSource_2013_Online_Fraud_Report.pdf?utm_campaign=Fraud%20Report%202013%20-%20Form%20auto-reply&utm_medium=email&utm_source=Eloqua

20 20131008-Cyberthreats-MultiplyingLikeTribbles-Report-pdf_3765_18213_10125_7966.pdf

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