TRANSACT 15 Show Floor Preview PAGE 28

March/April 2015

TRANSACTION *trends*

ETA THE OFFICIAL PUBLICATION OF THE ELECTRONIC TRANSACTIONS ASSOCIATION

Exclusive:
Read, Learn, and Earn ETA CE Credits
PAGE 32

Safe mode

Technologies and insights on the future of payments security

ALSO INSIDE:

Effecting Change With Policy Makers
PAGE 12

Tokenization Takes Center Stage
PAGE 14

How To Store Biometric Data
PAGE 22

Better ISO-Processor Communications
PAGE 36

Info Security Expert Brian Sadowski
PAGE 40

MAGTEK®
SECURITY FROM THE INSIDE

ACTION ITEMS:

- PREVENT DATA BREACHES
- ID COUNTERFEIT CARDS
- STOP FRAUD
- PROTECT OUR BRAND

SELL MORE. SAFER. FASTER. ANYWHERE.

with the DynaPro Family of Products

Recent data breaches make it clear that security and brand protection needs to be at the forefront of Point-of-Sale investments. With the need to future-proof equipment with new EMV requirements, PCI compliance, mobile POS convenience and NFC capabilities, it is important to select the right partner. MagTek has you covered with the most dynamic and flexible solutions and a variety of SDKs.

SUPERIOR TRANSACTION SECURITY

MagneSafe™ Security Architecture • Prevent Data Breaches • Identify Counterfeit Cards • Stop Card Fraud with the Global MagnePrint® Exchange

MULTI-FUNCTIONAL

Secure Magstripe • Signature Capture • EMV Contact/ EMV Contactless • NFC

FLEXIBLE CONNECTIVITY

iOS 30 PIN • Bluetooth 4.0 (BLE) • USB HID • Ethernet

DynaPro

DynaPro Mini

For more information about transaction security and protecting your brand, contact the MagTek Retail Solutions Team at 562-546-6400 | www.magtek.com

1710 Apollo Court I Seal Beach, CA I 90740 I 562-546-6400 I www.magtek.com

Each Click is a Residual Payment.

Authorize.Net has paid out more residual payments than any other payment gateway. Contact us to learn why.

Call 1.866.437.0491 or visit www.authorize.net

Authorize.Net®
a CyberSource solution

Now you know
PAX as a GLOBAL
PAYMENT LEADER...

...let us EASE your EMV TRANSITION

S80
Countertop

S90
Mobile

S300
Multilane

S500
Countertop

S900
Mobile

D200 Series
Wireless PINpad

Px Series
Multilane

Don't just take our word for it. Here are some **FACTS**:

- PAX is the **PCI, EMV** and **NFC EXPERTS**
- **LOCK TERMINALS** and future earnings
- Manage your **TERMINAL NETWORK** with ease
- Reliable, feature-rich, **COST EFFECTIVE** solutions
- **THIRD LARGEST POS** terminal provider in the world
- **INTEGRATED TERMINALS** to take POS/ECR systems out of EMV and PCI Scope
- Fully behind our products offering a **2-YEAR WARRANTY**
- **SIZE, STABILITY** and **TRUST, PAX** Delivers!

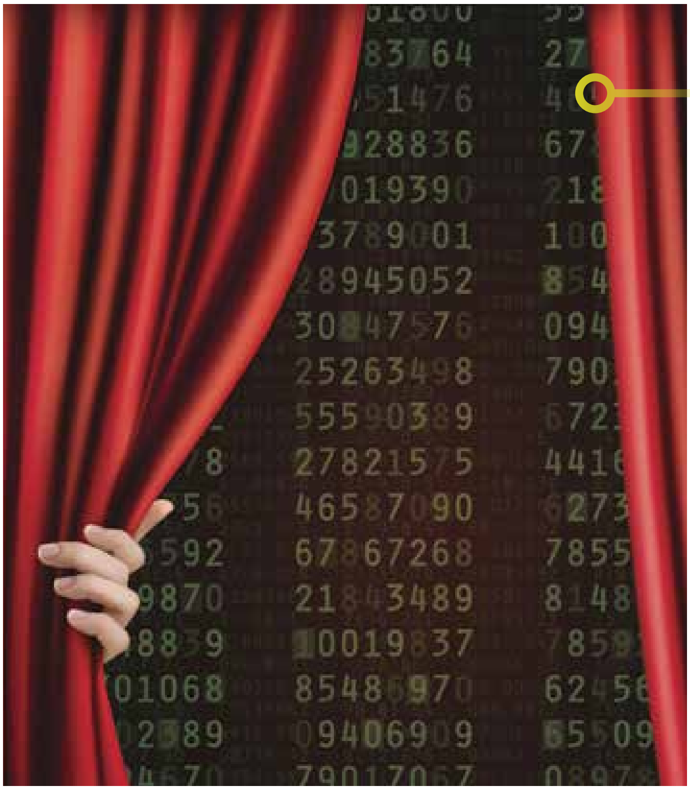
2 YEAR LIMITED WARRANTY

US HEADQUARTERS:
4901 Belfort Road, Suite 130
Jacksonville, FL 32256
+1-877-859-0099 | sales@pax.us

REGIONAL OFFICE:
40 West Baseline Road, Suite 210
Tempe, AZ 85283
+1-877-859-0099 | sales@pax.us

contents

The Official Publication of the Electronic Transactions Association Vol. 20 | No. 2



features

14 Tokenization's Starring Role
By Julie Ritzer Ross
As merchant adoption of tokenization solutions grows, experts explain how it will transform customer experience, security, and ubiquity—and how the industry still needs to develop a comprehensive standard and integrate it into existing processing practices.

22 At Home or in the Cloud
By Ed McKinley
As a backup security measure to Apple Pay, biometrics is getting attention. But opinion is divided on where to store the data. And, why has biometric authentication been slow to proliferate? Is some flaw holding it back, or is it an answer to a question no one is asking?

28 Show Time
What's new on the TRANSACT 15 tradeshow floor this year? A lot. From the Retail Technology Zone to the World of Bitcoin, this year's exhibit hall features something for everyone in the payments business.

32 *Transaction Trends* Exclusive CE Series: Breach Response for the Small Merchant
While large retailers get more attention for breaches, small merchants are the most common targets. Study these nine guidelines for helping your merchant clients create a data breach response plan. Then, take the online quiz to earn two CE credits!

departments

4 **@ETA** Announcements and ideas from ETA's CEO Jason Oxman

8 **Intelligence** Vital facts and stats from the electronic payments world

12 **Politics & Policy** Timely political, economic, and advocacy updates affecting your business

36 **Comments** How to fill the communications gap between ISOs and processors

38 **Ad Index**

40 **People** Data security is a moving target, says Brian Sadowski, who leads information security for Apriva's POS Gateway

Electronic Transactions Association
1101 16th Street NW, Suite 402
Washington, DC 20036
202/828.2635
www.electran.org

ETA CEO Jason Oxman

COO Pamela Furneaux

Director, Education and Professional Development Rori Ferensic

Director, Membership and Marketing Del Baker Robertson

Director, Communications Meghan Cieslak

SVP, Government Relations Scott Talbott

Director, Industry Affairs Amy Zirkle

Publishing office:
Content Communicators LLC
PO Box 223056
Chantilly, VA 20153
703/662.5828

Subscriptions: 202/677.7411

Editor
Josephine Rossi

Editorial/Production Associate
Christine Umbrell

Art Director Janelle Welch

Contributing Writers
John Manasso, Ed McKinley, Julie Ritzer Ross, Josephine Rossi, and Scott Talbott

Advertising Sales
Linda Baker
Advertising Sales Manager
Phone: 703/964.1240, ext. 13
Fax: 866/466.9187
Lbaker@conferencemanagers.com

Alison Bashian
Phone: 800/335.7500
Fax: 440/232.0398
alisonb@bashian.com

Editorial Policy:

The Electronic Transactions Association, founded in 1990, is a not-for-profit organization representing entities who provide transaction services between merchants and settlement banks and others involved in the electronic transactions industry. Our purpose is to provide leadership in the industry through education, advocacy, and the exchange of information.

The magazine acts as a moderator without approving, disapproving, or guaranteeing the validity or accuracy of any data, claim, or opinion appearing under a byline or obtained or quoted from an acknowledged source. The opinions expressed do not necessarily reflect the official view of the Electronic Transactions Association. Also, appearance of advertisements and new product or service information does not constitute an endorsement of products or services featured by the Association. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided and disseminated with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice and other expert assistance are required, the services of a competent professional should be sought.

Transaction Trends (ISSN 1939-1595) is the official publication, published six times annually, of the Electronic Transactions Association, 1101 16th St. N.W., Suite 402, Washington, DC 20036; 800/695-5509 or 202/828-2635; 202/828-2639 fax. POSTMASTER: **Send address changes to the address noted above.**

Welcome to the World's Largest Payments-Technology Event!

Welcome to TRANSACT 15: Powered by ETA! We celebrate ETA's 25th anniversary here in San Francisco—marking this milestone anniversary in our nation's hub of innovation. This week, thousands of payments and technology industry executives gather here to do business, explore technology innovations, and learn about new opportunities in commerce.

Worldwide, ETA represents more than 500 of the largest and most successful ISOs, acquirers, processors, and financial institutions, as well as the largest mobile network operators, technology companies, equipment manufacturers, security providers, and apps companies. TRANSACT 15 brings together payments and technology industry executives, venture capitalists, and media to see the next generation of payments.

TRANSACT 15 is the premier annual opportunity for expanding your payments business and connecting with your current and future customers and partners. Hear about the future of payments from keynote speakers Jingming Li, president and chief architect of Ant Financial Americas; Visa President Ryan McInerney; MCX CEO Dekkers Davidson; Frank Bisignano, chairman and CEO of First Data; and Doug Davis, senior vice president and general manager of the Internet of Things (IoT) Group at Intel.

We're presenting you with highest impact speakers and sessions, with six conference tracks featuring 59 educational sessions, and special highlights including Retail Solutions 2.0 and the EMV Bootcamp to ensure you are up to date on the latest payments intelligence.

For startups and industry veterans alike, our show floor is the marketplace for innovation. This year, we've added pavilions to highlight fast growing sectors of the payments industry. From the Payments NextZone to the Retail Technology Zone and World of Bitcoin, we provide an unequaled showcase for innovative payments industry products and services. (Read more about the show floor events on page 28.)

And the excitement goes beyond the show floor. Make sure to check out the Payments Pitch-Off that provides payments startups with the opportunity to compete for the $25,000 E-Pay Innovation Award, sponsored by Intuit. Contestants will demonstrate their innovative new electronic payments technology product or service to the payments industry's most important players.

We are grateful to our exhibitors, our sponsors, and our attendees for their support of this amazing event. I look forward to seeing you on the show floor as we explore new opportunities in payments. Thank you for being a part of TRANSACT 15. I look forward to growing our industry together over the next 25 years and beyond!

Jason Oxman
Chief Executive Officer
Electronic Transactions Association

Discover® is Partnering with the POS Channel to Accelerate EMV Deployment

Discover® is Engaged with the Channel on EMV

For the past several years Discover has been in discussions with key participants in the integrated Payments Channel in order to help plan for and accelerate EMV deployment. Discover has conducted EMV engagement discussions with the top ISVs in the channel in order to share information and validate EMV enablement plans. These ISVs account for the majority of merchants enabled within the POS ecosystem. These discussions have been beneficial to both parties as we have identified several ways to align interests and accelerate deployment of the Discover EMV specification called D-PAS. Discover recognizes that ISVs have a variety of solutions that they can explore to enable their merchant portfolios for EMV acceptance and this engagement has proven to be very valuable to our partners as they explore options including direct payments application integration, semi-integrated options, and solutions provided by Gateways and hardware providers. Discover has also participated on a series of EMV webinars within the channel, and most recently shared insights during an EMV Panel at RSPA INSPIRE 2015. http://www.bsminfo.com/doc/video-predictions-for-emv-in-and-beyond-0001

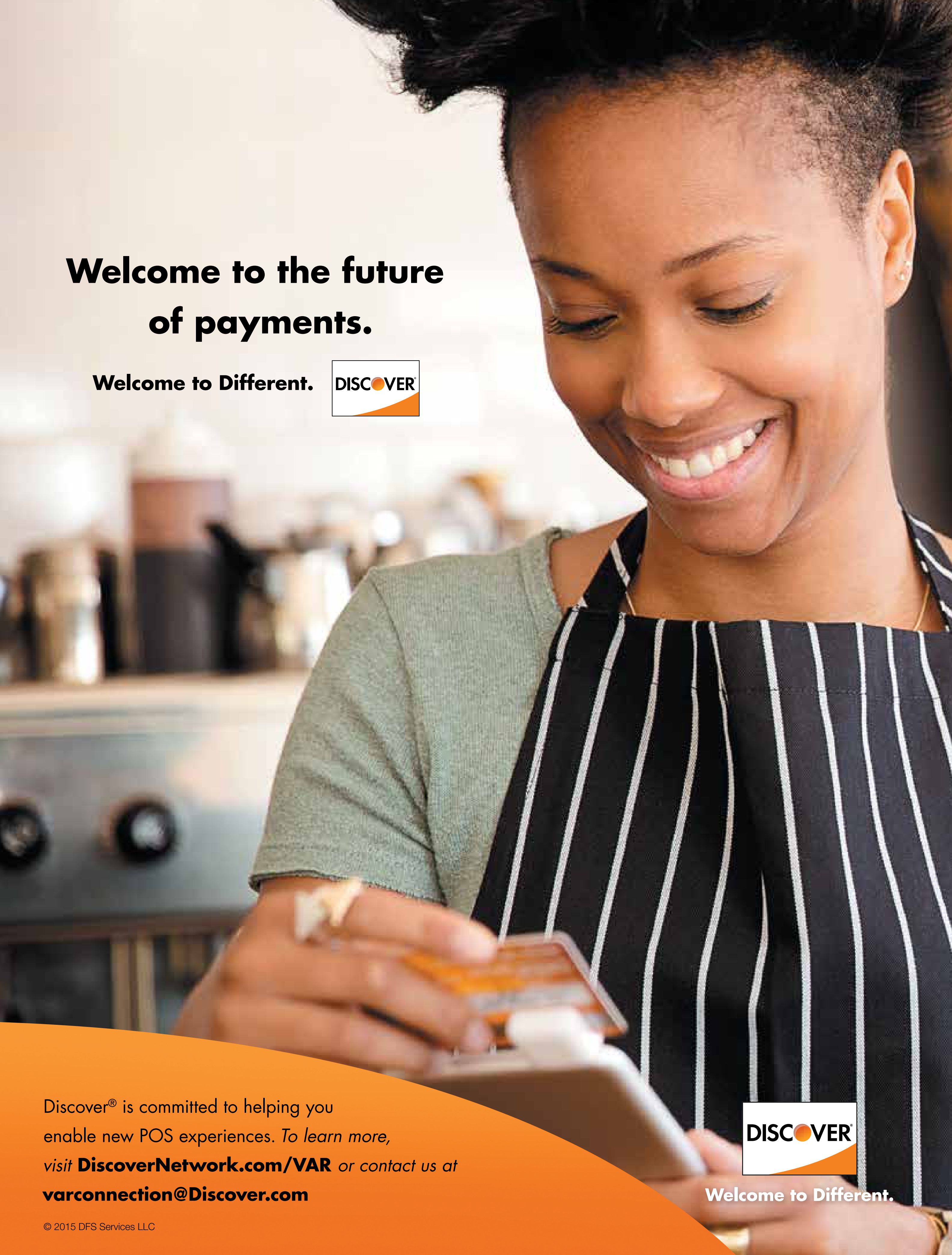
Discover Offers Resources for EMV Deployment

After listening to channel input, Discover has developed an engagement plan and resources that our channel partners can put to work to assist them in developing and deploying their EMV solutions. The Discover engagement plan helps to ensue ISVs help Discover achieve our objectives within the channel including: ensuring ISV applications enable the full set of Discover card ranges for transaction routing, engaging the ISV's Dealer network to educate them on Discover programs, and partnering to communicate Discover Acceptance at the cashier level. The greater the alignment of interests achieved with our ISV partners, the greater the resources Discover can make available to targeted partners. These resources include financial incentives for coding to support the Discover D-PAS EMV specification, access to third-party EMV certification tools to speed EMV card brand certification, and education support for rollout of the ISV's EMV solution to their Dealer base. Most recently we partnered with Digital Dining to help develop and accelerate EMV deployment. Andre Nataf, Senior Business Development Manager at Digital Dining said, "Digital Dining partnered with Discover early on in our EMV strategy development and we are pleased to have their support and resources as we now roll out our EMV solution later this month."

Discover is committed to celebrating partner's EMV Success

The channel's response to the Discover EMV engagement plan has been exceptionally positive. We are currently in EMV deployment discussions with the majority of our ISV partners, their Acquiring partners, and supporting Gateways. We look forward to celebrating and supporting these early deployments throughout the year both in the press and by partnering with engaged clients with whom we can promote mutual goals at industry events. To learn more about the Discover D-PAS EMV enablement resources please contact your Discover Relationship Manager. We are excited to share information and resources that support our common goals with D-PAS EMV deployment.

John Badovinac
Head of Integrated Payments
Discover Financial Services
2500 Lake Cook Rd.
Riverwoods, IL 60015
(800) 951-0633
DiscoverNetwork.com/var



2014: A ‘Mixed’ Year for Identity Fraud

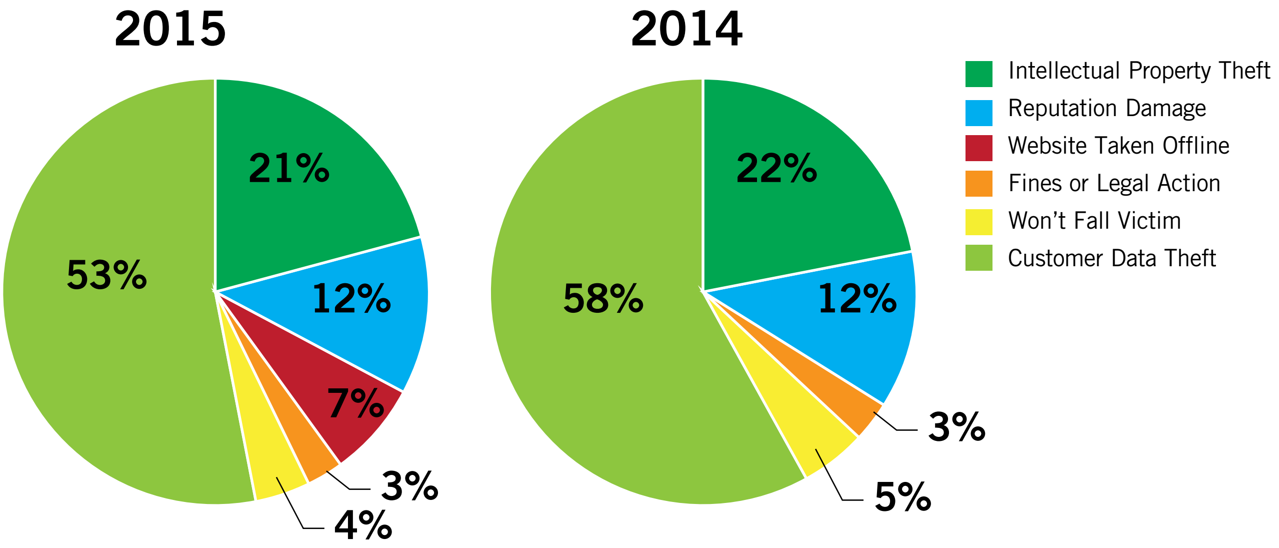
In the fight against identity fraud, 2014 had some advances and some setbacks. A new study by Javelin Strategy & Research found that fraudsters stole $16 billion from nearly 13 million U.S. consumers last year. With a new identity fraud victim every two seconds, consumers—particularly students—are still at significant risk, according to the survey of 5,000 U.S. consumers.

The 2015 Identity Fraud Study found several trends, including:

- Incremental decrease in victims doesn’t tell the whole story. The number of victims of identity fraud decreased by 3 percent from 13.1 million in 2013 to 12.7 million in 2014. But progress has been made with total fraud losses declining to $16 billion in 2014, a decrease of 11 percent from 2013 ($18 billion). Javelin attributes this to the combined efforts of industry, consumers, and monitoring and protection systems that are catching fraud more quickly.
- Students are least concerned, yet most severely affected, by fraud. Among several demographic segments analyzed, students indicated the least amount of anxiety about fraud occurring, with more than 64 percent saying they were not very concerned about fraud. Yet, this same group is more likely to perceive significant effects due to the occurrence of fraud (15 percent experiencing moderate or severe impact). Students are also the least likely to detect identity fraud themselves. Twenty-two percent of students were notified that they were victims of identity fraud either by a debt collector or credit denial, three times higher than average fraud victims. Students are also four times more likely to be victims of “familiar” fraud, versus all other consumers.
- Fraud victims avoid retailers. 2014 saw a significant amount of data breaches, most notably from retailers Neiman Marcus, Home Depot, Staples, and Michael’s, as well as financial institution JPMorgan Chase. These breaches had a great impact on consumer purchasing decisions, with 28 percent of fraud victims avoiding merchants post-fraud. Notably, individuals whose credit or debit cards were breached in the past year were nearly three times more likely to be an identity fraud victim.
- New account fraud goes undetected. New account fraud reached record lows in 2014, yet the study showed that victims are three times more likely to take a year or more to discover that their identities were misused compared to other types of fraud, such as existing non-card accounts. This can open the door for fraudsters to be able to use the victim’s identity for illicit behavior for a long period of time, which can result in greater harm to consumers in the form of financial losses, and problems with their credit history and scores.

Infographic

IT’s Top Cyberattack and Data Breach Worries 2015 v. 2014



Note: 2015 data from survey of 1,016 full-time IT professionals in the United States, Canada, and the United Kingdom.
Source: Trustwave, *2015 Security Pressures Report*

EVO® PAYMENTS INTERNATIONAL

NON-CASH PAYMENT SOLUTIONS AVAILABLE ANYTIME, ANYWHERE

As a leader in the payments industry, our mission is to forge partnerships through our innovative, reliable and secure payment solutions. We deliver value-added products and services and process over 50 billion dollars in transaction volume annually. These customized solutions reach more than 400,000 merchant businesses, in a variety of industries and sizes worldwide.

Our strong infrastructure and state-of-the-art payment platforms ensure safe and secure payment transactions, allowing us to provide the most advanced payment options needed in the market today.

> Card Processing Services
> Smart Mobile Payments
> Fraud & Security Prevention
> Risk Management
> Accelerated Funding
> Integrated Solutions

> E-commerce Solutions
> Cash Advancements
> Online Payment Acceptance
> Recurring Billing
> Merchant Reporting
> Gift and Loyalty

Smart partnerships build success.

Visit www.EVOpayments.com or call 1.800.227.3794
United States | Canada | Europe

More Research Shows Businesses Not Ready for EMV

Seventy-one percent of independent business owners are not aware that by October, Visa and MasterCard will hold them responsible for credit card fraud if they do not have a Europay/MasterCard/Visa (EMV) compliant terminal, according to Newtek Business Services Corp. This is the key finding its *Small Business Authority Market Sentiment Survey*, a monthly poll of more than 990 respondents.

Additionally, the February results showed that 81 percent of business owners have not yet upgraded their POS or terminal to be EMV ready and to accept Apple Pay.

"With approximately six months to go, it is still apparent that business owners still do not have a full understanding of the importance and issues surrounding the EMV strategy to accept chip card processing," said Barry Sloane, chairman, president, and CEO, in a press release. "We believe our data is skewed with a slight negative bias; however, as we go through our own database of customers, they are slowly moving over to EMV compliant merchant accepting platforms."

U.S. Millennials Will Embrace Nontraditional Banking Services in 2015

Not surprisingly, a survey of 908 U.S. bank customers conducted for FICO, the predictive analytics and decision-management software company, found that Millennials are embracing alternative banking services in greater numbers than older generations. Twice as many Millennial respondents (32 percent) report that they are likely to use mobile wallet services such as Apple Pay or Google Wallet in the next 12 months as those who are 35 and older (16 percent). Additionally, 56 percent of younger Millennials (ages 18 to 24) report that they are already using or very likely to use alternative payment services like Venmo and PayPal.

The survey asked respondents about their current and projected use of nontraditional banking services, such as mobile wallets, alternative payment services, and peer-to-peer lending. Among all respondents, 18 percent intend to use a mobile wallet in the next year; only 5 percent currently do so. Thirty-nine percent expect to use an alternative payment service in the next year, and 21 percent currently do.

"We already know that Millennials are inclined to conduct common banking activities through the digital channel," says David Vonk, who leads the North American banking practice at FICO. "While alternative banking may still be in its infancy, it has the potential to grow rapidly, especially as the Millennial generation enters its prime and pushes these services to the forefront of its banking agenda."

Fast Fact

Among the **40 percent of U.S. consumers who used mobile payments in 2013,** 45 percent used Google Wallet, 41 percent used a banking payment app, and one third used a retailer payment app.

Source: Walker Sands, *Future of Retail Study 2015*

ETA'S ADVOCACY EFFORTS YIELD A NUMBER OF SUCCESSFUL OUTCOMES

Moving the Needle

By Scott Talbott

As the world's largest payments industry trade association, ETA is the industry voice, heard both in Washington and in state capital cities nationwide.

ETA is the leading organization advocating for the payments community. Having a voice in politics is crucial for businesses of all sizes. At a time of unprecedented change in the payments industry, ETA's government relations efforts are enormously important to our industry. Federal and state policy makers have a huge impact on how we do business—and this influence is only growing stronger.

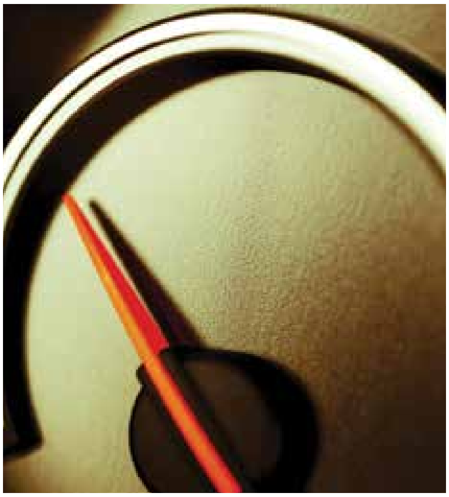
Now that the 114th Congress is in full swing, I am pleased to share the highlights of our recent advocacy initiatives in addition to a preview of what may be in store for the payments industry in the months ahead.

Operation Chokepoint

Operation Chokepoint (OCP) is an effort by the Department of Justice (DOJ), Federal Trade Commission (FTC), and Federal Deposit Insurance Corporation (FDIC) to reduce consumer fraud by holding banks and processors liable for the fraud committed by merchants. OCP emerged as a regulator-led effort to target certain types of merchants such as payday lenders, pawn shops, and handgun and ammunition sellers. There was wide concern in the payments industry, and within those targeted industries, about government overreach and potential impact to lawful participants of the payments system.

Last year, ETA led the charge in pushing back against OCP. To date, we have seen a large measure of success, including the following:

- FDIC has issued a letter to all banks encouraging them not to de-risk merchants by category.



- FDIC has officially withdrawn the list of objectionable industries.
- Attorney General nominee Loretta Lynch and CFPB Director Richard Cordray have distanced themselves from the effort.
- Internal investigations have been opened at the DOJ and FDIC for abuse of authority.
- Legislation has been reintroduced to prohibit bank regulators from targeting lawful businesses.

These steps are encouraging, but ETA will remain vigilant during 2015, keeping the pressure up and continuing to utilize the ETA Guidelines as an example of how best to reduce and eliminate fraud.

Cybersecurity

The hacks of Sony, Anthem, and some foreign banks, and more than 70,000 attempts to hack the federal government last year, have made cybersecurity a top priority in Congress. For ETA, there are two main priorities: data breach and information sharing. So far during 2015, Congress has held numerous hearings and reintroduced a number of bills. The president has issued suggested language in both areas.

In terms of data breaches, given that most ETA members operate in multiple states (and many operate in all 50 states), ETA has strongly supported the creation of a uniform national standard for breach notification. There is a groundswell of support for making such a standard law this year. ETA will continue to press for it, using direct lobbying and grassroots efforts.

Regarding information sharing, ETA strongly supports removing restrictions and allowing private companies and the government to share information about cyberthreats. ETA will continue to press for information sharing legislation.

Progress With Lawmakers

ETA has been busy working with national and state legislators on a variety of important issues.

Recently, ETA helped organize a new bipartisan Congressional Payments Technology Caucus. The Caucus is chaired by Reps. Lynn Westmorland (R-Georgia), Chairman Randy Neugebauer (R-Texas), and David Scott (D-Georgia). The purpose of the Caucus is to bring together those members of Congress who understand the issues facing the payments technology industry. ETA plans to provide quarterly briefings on timely topics to the Caucus. The Caucus is open to all members of the House of Representatives, and a kick-off reception is planned for April 30.

ETA also is staying active with state capitols and regulators. Below is a summary of key efforts so far during 2015:

Washington State: The Department of Revenue is taxing interchange as if it were revenue to processors. ETA opposes this initiative and organized a group of companies and local experts to meet with the acting director of the Washington State Department of Revenue on March 16 to express concern about the application of the business and occupation tax to processors' interchange volume.

Colorado/Nebraska: Both Colorado and Nebraska saw legislation introduced to prevent the application of interchange to the sales tax portion of a sale. ETA joined forces with state banking agencies and opposed both bills. The Colorado bill has been converted to a study, and the Nebraska bill is not projected to move.

Puerto Rico: ETA is working on pushing back against Puerto Rico's new 2 percent tax on money transfers. The organization is helping individual ETA member companies request extensions of the time to be subject to the new tax and is leading an effort to move legislation to repeal the tax or carve out affected ETA members. As a last resort, ETA may file a lawsuit to challenge the new law.

Cuba: Last December, President Obama took steps to normalize relations with Cuba, including allowing U.S. payments companies to do business in Cuba. During 2015, ETA is working with the Departments of State and Commerce, as well as the Department of Treasury, to assist in the implementation.

Prepaid Cards

In addition to Congress, federal and state regulatory bodies have the ability to dictate policy that affects how ETA members conduct business. During 2015, ETA is engaging with federal and state regulators to advance the payments industry's positions.

The Consumer Financial Protection Bureau (CFPB) released an 870-page proposal to regulate general reloadable prepaid cards. The proposal would create heavy regulatory burdens on mission-critical features of prepaid cards, including overdraft, and create confusion for consumers with disclosure requirements. The proposal also attempts to regulate peer-to-peer lending, mobile transactions, and Bitcoin. Comments were due on March 23.

ETA's position is that we are very concerned that the proposal will greatly reduce the availability of prepaid cards, or some of their features. ETA is working with Congress and the CFPB to express concerns about the breadth and depth of the proposed burdens. So far this year, ETA has taken the following steps:

- Hosted ETAU on March 19 with four prepaid companies (Netspend, FirstData, Blackhawk, and InComm), discussing the issue before 50 Hill staff.
- Met with the relevant congressional committees to discuss ETA's concerns.
- Created a working group to file a formal comment letter to the CFPB.
- Formed a joint trade association to share arguments and coordinate the response.
- Met with the leadership and staff of the CFPB.

Politics is not a spectator sport, so we encourage you to get involved with ETA as it represents the payments industry. Our new political engagement program, ETA Voice of Payments, gives you the tools necessary to ensure elected officials hear the voices of their constituents on issues of importance to the $5 trillion payment processing industry. Please visit http://voiceofpayments.org/ and start participating today. ***TT***

Scott Talbott is senior vice president of government affairs for ETA. Reach him at stalbott@electran.org. For more information, contact Jaime Graham, senior manager of government affairs, or Grant Carlson, government affairs coordinator, at 202/828.2635.

Tokenization's

As merchant adoption increases, tokenization becomes more than a bit part in the security scene

By Julie Ritzer Ross

As the drama and deadlines for Europay/MasterCard/Visa (EMV) continue to heat up, those who are unfamiliar with the payments profession may assume that improving data security ends with the October shift to the EMV standard and merchant adoption of EMV-compliant POS technology. Not so. Tokenization also is making its mark—not only with issuers and acquirers, but also with merchants.

In a nutshell, tokenization entails replacing a high-value credential (the primary account number (PAN) on credit cards) with a unique, randomly generated sequence of numbers, alphanumeric characters, or a combination of a truncated PAN and a random alphanumeric sequence. This makes sensitive data worthless to hackers and other perpetrators. Tokens can be either single- or multiple-use and may be reversed to their true associated PAN value at any time with the proper encryption keys.

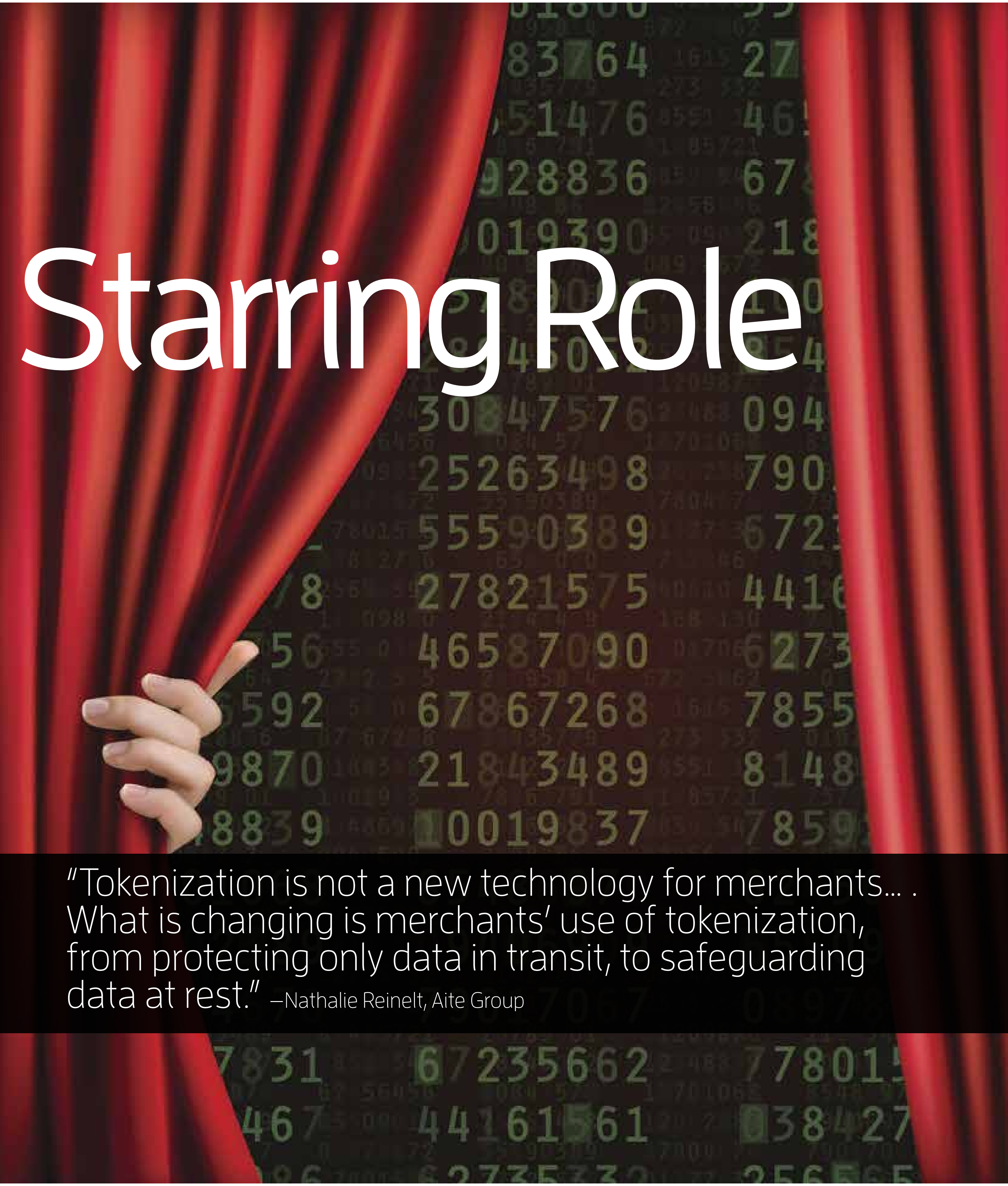
"Tokenization is not a new technology for merchants; they have deployed it in their environments for quite some time," says Nathalie Reinelt, an analyst with research firm Aite Group. "What is changing is merchants' use of tokenization, from protecting only data in transit, to safeguarding data at rest. The recent data breaches have highlighted remaining vulnerabilities that need to be addressed—namely, ensuring data is tokenized as soon as it hits merchants' systems and at the front and back ends alike."

The proof is in the numbers. Of merchants surveyed by Aite Group in 2014, 44 percent reported that they utilize tokenization, and 22 percent noted that it is on their "one- to two-year roadmap." An additional 3 percent of participants cited plans to harness tokenization technology at some point, but not in the next two years, leaving just 13 percent of merchants queried with no intentions of introducing tokenization in their organizations.

A study conducted late last year by technology research firm IHL Group and *RIS News* magazine uncovered similar data. Thirty percent of U.S. merchants have adopted tokenization, and another 27 percent plan to do so this year.

By Gartner Research's estimates, 50 percent of Level 1, Level 2, and Level 3 merchants combined have some form of tokenization technology in place or will do so in 2015,

Starring Role



"Tokenization is not a new technology for merchants… . What is changing is merchants' use of tokenization, from protecting only data in transit, to safeguarding data at rest." –Nathalie Reinelt, Aite Group according to Avivah Litan, distinguished analyst and vice president. Meanwhile, last year, the PCI Security Standards Council (PCI SSC) commissioned a survey of 700 of its members in an effort to "understand the current state of tokenization, focusing solely on tokens used by merchants and acquirers for data-at-rest security purposes." Conducted by Glenbrook Partners, the survey revealed that while tokenization for data-at-rest security purposes is not ubiquitous, it is "widespread," with 50 percent of top-tier merchants in the United States and United Kingdom currently using it, and 20 to 30 percent of lower-tier merchants doing the same.

> "BY TOKENIZING DATA, A MERCHANT MIGHT BE ABLE TO REMOVE A HUGE AMOUNT OF THE IT INFRASTRUCTURE PORTION OF ITS PCI AUDIT, RESULTING IN SIGNIFICANT FINANCIAL SAVINGS."
>
> —Richard Moulds, Thales e-Security

Spotlight on Value

Merchants' perceptions about the efficacy of tokenization may be a catalyst for the adoption rates. Of merchants polled by Aite Group, 50 percent characterized tokenization as having a "high" (31 percent) or "very high" (19 percent) effect on fraud and data security.

Recognition among U.S. merchants that tokenization offers a high value proposition also is bolstering acceptance, on several levels. For online merchants, it's ammunition against fraudsters, whose attentions are shifting from the card-present environment to card not present (CNP) as migration to EMV-ready terminals protects bricks-and-mortar retailers from data breaches. Current forecasts call for a sharp uptick in CNP fraud over the next few years, with Javelin Strategy & Research predicting it to be four times greater than POS card fraud in 2018 regardless of EMV adoption. (Get the data on how EMV has affected CNP fraud in other countries in the January/February issue of *Transaction Trends*.)

"EMV does not necessarily solve CNP-related fraud; it may actually increase the possibility," says Andrew Luca, co-leader of the U.S. Payments Practice at PricewaterhouseCoopers and a partner in the firm's Advisory Financial Services, Banking Strategy Technology and Operations Practice. As more merchants become EMV-compliant, CNP retailers become prime targets for attack.

Equally compelling to merchants is the potential to reduce scope of compliance with the PCI Data Security Standard (PCI DSS), which covers only those systems that are exposed to unaltered cardholder data—namely, POS devices, servers, and databases. If a merchant's systems are only exposed to tokenized cardholder data, the systems are out of scope and need not be assessed for compliance with the standard. "By tokenizing data, a merchant might be able to remove (be exempt from) a huge amount of the IT infrastructure portion of its PCI audit, resulting in significant financial savings," explains Richard Moulds, vice president, product strategy, Thales e-Security. Further, this benefit applies as much to bricks-and-mortar merchants as it does to CNP merchants.

Similarly, tokenization addresses vulnerabilities in the application layer of merchants' systems, where the majority of threats are said to reside. Findings of a study conducted by Verizon's RISKS Team computer forensics practice demonstrate that 92 percent of all data breaches are the work of external agents, who primarily target servers and applications. Servers accounted for 80 percent of breaches and 95 percent of compromised records cited in the study, with POS servers and web servers leading the pack on both sides.

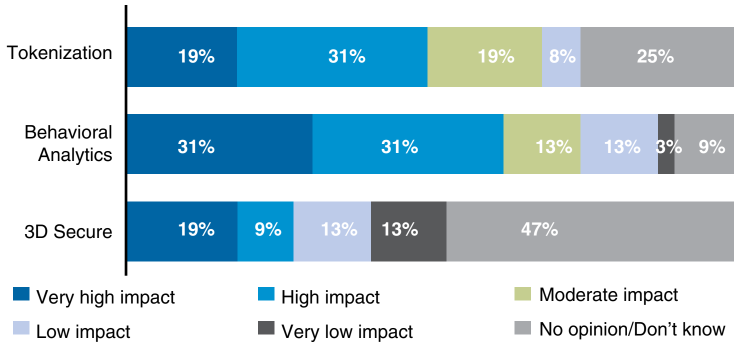
Traditionally, a combination of encryption and strong key management has been the favored method of enforcing data protection in applications. However, in addition to what some sources characterize as a "dramatic" reduction in security and compliance requirements and costs, merchants are now compelled by the fact that tokenizing sensitive data in the application layer (removing data from systems and applications that do not require it) necessitates only minor, relatively inexpensive application changes. Encrypting that same data, however, is typically a slower, more expensive process.

Then, there is the allure of different use scenarios. Consider merchants that need to retain customers' credit card information for monthly subscriptions or recurring bills. If such information is tokenized, recurring and/or future-dated transactions may be set up without incurring the cost, risk, and liability of storing sensitive data in-house—creating an "ideal solution" for merchants, says Jeff Thorness, CEO, Forte Payment Systems.

Another example is predictive analytics initiatives. The adoption of an omnichannel business model is driving merchants to capture and retain massive amounts of sensitive data, and to apply predictive analytics to provide the highly personalized levels of customer service. The "best" analytics will include personally identifiable information (PII) as well as location, transaction, and other sensitive data, which responsible merchants now acknowledge should be de-identified as close to the source of acquisition as possible so it is "protected wherever it goes in the ecosystem and throughout its lifecycle," says Carole Murphy, director, product marketing, Voltage Security.

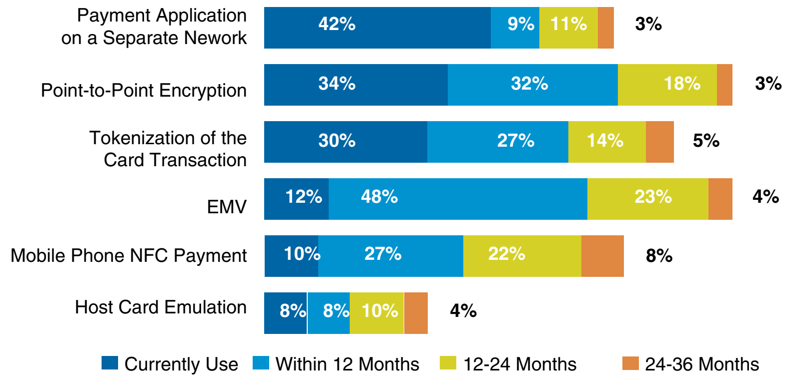
Tokenization also can be used to protect "other types of sensitive data, beyond financial," observes Rob Sadowski, director of technology solutions at RSA, a provider of Cloud-based data security solutions and services. He puts PII, which must often be disclosed by merchants in the event of a data breach, on the list.

Perceived Effectiveness of Security Solutions



Source: Aite Group, *EMV Lessons Learned and the U.S. Outlook, 2014*
Note: Information gathered from a survey of 36 merchant fraud executives, March to May 2014

Card Security Adoption



Source: RIS News, *Store Systems Study, 2015*

Merchants have come to the "swift realization" that reducing the surface area of sensitive data within their systems is the only rational approach to protecting their vast reserves of PII data (along with PCI data), says Ulf Mattson, chief technology officer of Protegrity, a provider of enterprise data security software and solutions. By some estimates, he says, users of tokenization for both PCI and PII data experience up to 50 percent fewer security-related incidents—specifically, unauthorized access to data, data loss, and data exposure—than users of other protective options.

Future Focus

Still, some other issues must be addressed before merchants' use of tokenization solutions becomes ubiquitous. Many industry players consider standards to be particularly important, in part because they offer merchants (and other stakeholders) a reliable framework for making decisions about token formats, replication, and other key matters.

Tokenization models are currently being developed by a variety of entities, including EMVCo, The Clearing House, card networks, and the ANSI X9.119 working group. However, the question of how these standards may complement each other—especially as they move through different stages of development and coordination—remains unanswered. To complicate matters, the models do not have consistent terminology, which is a must for the creation of common standards.

"The standards that have been proposed so far have been so convoluted that we don't see much benefit in them," says Dave Oder, CEO, Shift4 Corp. This will need to change to get more merchants on board with tokenization.

Interestingly, the PCI SSC had intended to publish a standard for tokenization, but has changed its direction based on feedback from the market survey. In addition to gaining a better understanding of the current state of tokenization as applied to data at rest, the Council's intention in conducting the survey was to assess the market's support for standardization, best practices, and other services around tokenization, especially PCI validation of token-generation software. "It became clear that acquirers and merchants generally support our development of a validation and listing process for vendor and commercially operated token generation, and that because of pre-existing deployments, 'best practices' around a risk-based approach were more desired," says Troy Leach, chief technology officer.

The Council will publish *Tokenization Product Security Guidelines*, a compilation of best practices, this spring. For merchants, it will address a multitude of concerns, including which criteria to apply when evaluating commercial tokenization solutions and how to test solutions for generating their own tokens.

The Council also is working closely with EMVCo on its tokenization framework and assessing whether there is a need for a PCI to complement it, according to Leach. Survey participants, he says, clearly indicated an interest in seeing the Council step into a coordinative role in conjunction with other standards bodies in the tokenization space.

Efforts by acquirers and software developers to offer better, more comprehensive tokenization solutions are equally critical to merchant acceptance. Sources say solutions that incorporate tokenization, P2P encryption, and EMV fall into this category, given that true data security can be accomplished only if all three are part of merchants' technology toolbox.

"What needs to be done—and what we are beginning to see some acquirers do—is to package, for merchants with standalone terminals, solutions that support EMV, encryption, and tokenization of data in motion and at rest," says Chris Bucolo, senior manager of partner relations for the security and compliance practice at Sikich LLP, a multidisciplinary professional services firm. "These combined solutions aren't going to suit every need, but there is plenty of room in the marketplace for them."

Tokenization solutions also should facilitate implementation and use on the merchant side. Take format preservation encryption (FPE), suggests Don Weary, vice president, product management, Sage Payment Solutions. FPE allows data-level encryption to be integrated into legacy business application frameworks that, prior to its advent, were difficult or impossible to address. With FPE in place, data retains its original format, eliminating the need for database and application schema changes.

"Format preservation makes existing systems more acceptable, but software vendors need to appreciate the value of security and invest in the technology to deliver format-preserving tokens," says Weary.

Similarly, tokenization solutions should not force significant changes to existing systems and business practices. Sources claim solutions that have been most widely deployed to date make adoption easy by building tokenization into existing transaction processing flows and require little or no modification to store and back-office systems, including, but not limited to, POS, loyalty, and analytics.

Finally, some experts believe regulations will be a tipping point for merchant-level tokenization of all data, at rest and in motion alike. "What is happening with EMV adoption and the liability shift is a good example (showing) that adoption (will move forward) when forced by regulations, compliance, and executive orders," Luca asserts. "It will happen—maybe not as fast as we would like—but it will happen." ***TT***

Julie Ritzer Ross is a contributing writer to Transaction Trends. *Reach her at jritzerross@gmail.com.*

PLANET Group Inc.

Acquire360

Complete Merchant Settlement, Accounting and Exception Management System

Take control of backend processing with Planet Group and Acquire360!

- Differentiate your business
- Control costs
- Improve earnings, market share and valuation

Contact us today to take control with Acquire360
and be your own processor!

Support for all major card types and multi-currency, including:

VISA MasterCard DISCOVER AMERICAN EXPRESS $ € £ ¥ ₩

PLANET Group Inc.

+1.800.979.9166

planetgroupinc.com
info@planetgroupinc.com

At Home or in the Cloud

By Ed McKinley

More than a century after Sherlock Holmes began using fingerprints to solve fictional crimes, the swirls and whorls on fingertips are authenticating transactions on smartphones in real life. But opinion remains divided on where to store the biometric data—locally or in the Cloud.

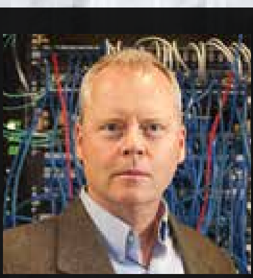
It's an important question because the number of biometrics smartphone users in the world is expected to reach 471 million in 2017, up from 43.23 million in 2013, according to a Frost & Sullivan report called *Biometrics Go Mobile: A Market Overview*. And the answer depends on how well vendors store information in the Cloud.

Some payments industry security experts feel comfortable warehousing biometric information in depositories outside consumers' devices as long as it's handled with the utmost caution to guard against theft. Safeguards can include capturing multiple data points to describe the fingerprint, thus making it difficult or at least too expensive

Should the payments industry store biometric data on smartphones or in hosted depositories? It all depends…

Chris Bucolo, Sikich

Daniel Martin,
ControlScan



Gary Glover,
SecurityMetrics

Greg Rosenberg,
Trustwave

Marc Castrechini,
ETA CPP, Cayan

Steve Robb,
ControlScan

to duplicate, says Gary Glover, director of security assessments for SecurityMetrics, a security vendor.

Strong encryption, tokenization, and firewalls—the security technology that protects card transactions—also can help keep biometric data safe in the Cloud, notes Chris Bucolo, senior manager of partner relations for the security and compliance practice at Sikich LLP, a professional services firm.

How well and how often the host performs scans and penetration tests also can prove crucial to the safety of Cloud storage.

The PCI Security Standards Council (PCI SSC) has issued guidance on Cloud computing and Cloud service providers. Security professionals should perform scans quarterly and penetration tests annually, whether the data is in the Cloud or not, according to spokesperson Laura Johnson. They also should employ both procedures anytime the site changes significantly, she says.

> THE U.S. MILITARY AND FEDERAL AGENCIES ARE INVESTING IN THE TECHNOLOGY, TOO, INCLUDING USE OF "INVISIBLE" PATTERNS LIKE TYPING SPEED AND OTHER PERSONAL HABITS TO IDENTIFY USERS.
>
> —Chris Bucolo, Sikich

The way the tests are conducted and who performs them depends on the relationship and agreements between the site operator and security vendor. "So it's important for organizations to evaluate and understand the risks and compliance implications unique to each deployment scenario when determining the best approach," says Johnson.

Using biometrics can add a layer of security to the password, PIN, or behavior-pattern recognition that a system already uses, which makes the transaction and the consumer's identity that much more secure, says Glover. Plus, counterfeiters find it more difficult to steal a fingerprint and fabricate a fake thumb than to guess a weak password or make a videotape of a victim punching a PIN number into an ATM.

What's more, crooks seem unlikely to invest much time or effort into pursuing biometric data because a successful theft would yield a single identity. They prefer to highjack thousands they could sell wholesale online or sort through to find the few with truly high credit limits.

It's even possible to store a fingerprint in a "one-way hash" that makes it nearly impossible to unwind the data and return it to its original form, says Marc Castrechini, ETA CPP, vice president of product management at Cayan LLC, an ISO and tech company that recently changed its name from Merchant Warehouse.

Keeping Data Earthbound

But even though companies that do everything right can safely store biometric data in the Cloud, some experts would prefer to confine the information to smartphones. The devices themselves can contain a secure computing element—a dedicated chip or a hardened storage facility—intended to make breaking in difficult and expensive.

"(The secure element) is what a lot of people have been waiting for when it comes to storing PPI—private personal information," says Greg Rosenberg, a security engineer at Trustwave, a security provider.

Many consumers find local storage more comforting than keeping data in the Cloud, according to Castrechini. In fact, he sees no need to resort to Cloud storage. "Biometrics works really well as an identification or authentication mechanism. For that reason, we believe it should be controlled by the owner."

Yet whether the data stays home on a smartphone or floats up to the Cloud, merchants often seem averse to adopting biometrics. "You have to make the business case," says Rosenberg. "What's the compelling use, and how do we do it in a cost-effective manner?"

Moreover, many consumers—especially older ones—balk at giving up their fingerprint to an outside entity. For some, it just seems too personal. Others can't shake unpleasant associations with crime, arrests, and mug shots.

Then there's the finality of fingerprints. Consumers can't simply get a new one if a crook succeeds in stealing one. "If someone exploits a vulnerability somewhere and gets your biometric information, they can become you," says Steve Robb, senior vice president at ControlScan, a security provider. "It's hard to recover from that without moving into some other security scheme."

That's why it's important to remember that some companies don't actually store the entire fingerprint, say experts. While some take a photo of the fingerprint, others create a matrix of points on a grid or a mathematical version of the electrical conductivity of the finger.

Consumers who hesitate to surrender their fingerprint could find solace in the way Apple keeps biometric data within their control. With Apple Pay, the authentication occurs inside the smartphone instead of comparing data stored in two locations after giving up biometric data to corporations, sources say.

Apple emphasizes in its marketing campaigns that the iPhone 6 reader does away with the need to reveal card numbers, security codes, or even consumers' names. "This additional layer of privacy helps ensure that your information stays where it belongs. With you," the Apple site says to reassure users.

"Seeing how well it works on the Apple phone, I like it," says Glover. "I don't have to type in my password when I buy an app. I just hold my finger there and it works—for convenience it's awesome."

The system's a vast improvement over the annoyingly inconsistent scanners of a decade or so ago, experts agree. The scanners attached to personal computers and read a swiped fingerprint for online purchases. "I remember getting a laptop a couple of years ago, and it had a fingertip reader built into it," says Robb. "It probably worked about once out of every four times I swiped my finger."

Conceding Perfection

But the iPhone 6 system isn't flawless. Glover found that his worked well for a month but then began having problems because a "small amount of gunk on the fingerprint processor" got into the home button, he says. Since then, he's been keeping the apparatus clean.

Later, when Glover exposed the smartphone to an RFID signal that reads lift tickets on a Utah ski slope, the device activated itself and began trying to make a payment with his American Express card. "I know what's going on, so it doesn't bug me a lot," he says of the incident. "But somebody else might see that and say, 'I'm going to turn this Apple Pay thing off.' "

With the proliferation of RFID readers—they do everything from granting employees access to the workplace to shortening lines at sporting events—Glover is not alone in having what he calls a "funky" experience: A paper cut on Robb's index finger prevented a Samsung Galaxy smartphone from reading his fingerprint.

And no system offers 100 percent protection from data thieves. "It's kind of like a car alarm," says Daniel Martin, ControlScan director of IT security and compliance. "It's a deterrent. If they really want to steal your car, they're going to get it whether you have a car alarm or not."

But for the most part today's technology is working, and the industry is apparently narrowing its focus to fingerprints as opposed to other types of biometrics.

Meanwhile, Visa is giving biometrics a boost by stipulating that contactless acceptance accompany the shift to Europay/MasterCard/Visa (EMV), Rosenberg says. Liability for breaches that EMV could have prevented shifts to merchants that don't accept chip cards in October. "That at least allows the possibility for acceptance" of biometric authentication, he says of the decision to include contactless payments in the transition to EMV.

Once that opportunity exists, a giant retailer like Walmart can advocate using the technology, and much of the world will follow, Bucolo says. Much of the impetus for adoption could come from consumers because younger people—unlike many of their elders—will appreciate the aura of biometrics and feel comfortable with it, says Glover.

Meanwhile, the recent rash of data breaches has prompted legions of biometrics companies to enter the market. The U.S. military and federal agencies are investing in the technology, too, including use of "invisible" patterns like typing speed and other personal habits to identify users, says Bucolo. That influx of companies and government bodies is forming a big fragmented biometrics market that's typical of U.S. business, he says, adding that with their varied approaches to biometric issues, those companies and agencies could give rise to standards or federal regulation.

"It certainly would behoove us to come up with a standard," agrees Castrechini. "If there isn't a mechanism protecting the data, ultimately business entities can do what they want."

The FIDO Alliance, short for Fast Identity Online, is developing specifications to change online authentication by combining biometrics with other methods, says Bucolo. One goal is to eliminate passwords.

The Cloud Security Alliance has come into being and has signed up 48,000 members worldwide, according to published reports. Biometrics for eCommerce, a LinkedIn group, also is sharing information, according to Bucolo.

Alternatives to Fingerprints

As the payments industry moves toward biometrics, it's focusing on fingerprints instead of other types of physical data—all of which have drawbacks.

Biometric alternatives include recording the unique array of finger lengths on a hand, which theme parks use, but that could require more space than the screen of a smartphone.

Facial recognition marks the unique distances between features like eyes and lips, and it's become familiar through Facebook tagging. But it may go asunder with an image captured at a weird angle or in poor lighting.

Retina scans would provide plenty of data, but thieves who manage to take high-resolution photos of their victims could counterfeit the information.

Voice patterns worked well as identification technology on *Star Trek*, but in real life, background noise may interfere. Wrongdoers could record conversations and duplicate the patterns.

What about shining a bright light at a hand to reveal the patterns of the capillaries or run an electrical pulse through the hand to detect unique qualities? Both would require laboratory conditions.

Cardio rhythms also could authenticate users, but may take too long to capture.

It's a lot to digest, but ISOs shouldn't become discouraged and disregard biometrics, security experts advise. "ISOs and acquirers should be keeping abreast of what's going on and should understand the issues," says Bucolo. "They should have a voice in the process and make sure their needs and their concerns are being represented."

ISOs need that knowledge and can benefit from participating in a switch to biometrics because it will be their job to advise merchants on how to deal with the technology, says Castrechini.

But when ISOs spread the word on biometrics they may encounter tough resistance from small and medium-sized merchants that have already invested recently in EMV readers, encryption, and tokenization, says Martin. And many smaller merchants may now fear the world of payments is bypassing chip cards in favor of smartphone transactions authenticated partly through biometrics.

However, some view those merchants' fears of biometrics supplanting EMV as misplaced, according to Castrechini, who says the two types of technology can coexist: "We don't foresee ubiquity for biometrics. It will just be some portion of the market. We would like to see EMV and biometrics layered. There's an opportunity for all of the technology to converge to come up with the best solution."

That varied approach to authentication shouldn't prove too complicated for merchants and consumers because both groups are becoming more security-conscious because of breaches and the publicity surrounding Apple Pay, says Castrechini. "Consumers are starting to show a preference for the more-layered forms of security. Merchants are starting to poke and probe into more advanced approaches."

No matter what direction payment security takes, biometrics alone just isn't enough to authenticate transactions safely, according to Rosenberg. "I wouldn't view biometrics, just by itself, as some sort of silver bullet for authentication," he says. "You have to consider what constitutes a biometric solution and whether it's something you're comfortable with."

In other words, not all biometrics are created equal—whether they're stored locally or in the Cloud. ***TT***

Ed McKinley is a contributing writer to Transaction Trends. *Reach him at edmckinley773@yahoo.com.*

Sponsored Content

Put Your Apple Pay Merchants On The Map With The Pay Finders App

The rapid expansion of NFC is now become a reality. With Apple Pay, Samsung Pay and Android Pay it is clear there will be no end to this growth. Apple Pay is leading this charge for a number of reasons and all experts predict that Apple will lead this revolution for some time.

The challenge for Apple Pay over the next few years is letting very willing users know where they can discover merchants that have NFC devices. Our solution has produced the largest human curated map of merchants using NFC in North America. We have built a number of unique systems that makes Pay Finder not only the largest NFC map available but also far more accurate.

Put your merchants on the map. There will never be a cost to you you, the merchant or the user for Pay Finders apps or maps. Merchants can claim existing locations and to update the accuracy of the listing. At Pay Finders since we are not affiliated to any brand, network, processor or ISO we can be assured of the largest number of merchants listed.

There is simply no reason not to put your Apple Pay merchants on the Pay Finders app. Help us build the largest Apple Pay map in North America and Pay Finders will help build more traffic to your merchants.

Please visit **http://www.PayFinders.com/MapBuilders** or **MapThis@PayFinders.com** or call 415 881 7283.

www.nuspay.com

nuspay
My Secret, My Freedom

VIRTUAL ACCOUNT– TOKENIZED PAYMENT SOLUTION.

Your life is invaluable, as are your transaction details. So, when your payment transactions pose threats of hacking, it is necessary to ensure that your financial information is not compromised. Nuspay has developed a unique tokenized Virtual Account solution that successfully addresses the issues of Global Payment Fraud. Actual financial details of customers are never required for any transaction and a short lifespan of the Virtual Account payment token eliminates much of the transaction fraud and hacking risks. We guard your financial details, so your financial security is ensured.

Cashless

Cardless

Contactless

Nuspay has developed a unique payment technology, filed for the patent and successfully published it on December 4, 2014 (Pub. # US 2014/0358783 A1).

We have also developed and accommodated other embedded payment solutions to work as a microfinance payment service provider.

TRANSACT® 15
POWERED BY ETA

CONNECTING THE PAYMENTS TECHNOLOGY WORLD

Show Time

TRANSACT 15 features innovation at every turn, starting on the show floor

The payments landscape continues to change at breakneck pace, with new technologies emerging and players converging at every turn. Remaining abreast of these developments, as well as networking with other industry stakeholders and exploring new partnerships, remains imperative to navigate such change and maximize the growth potential it affords. Participation in TRANSACT 15 is a critical step in the right direction.

TRANSACT 15 is much more than an annual conference. From March 31 through April 2 at Moscone Center in San Francisco, ETA is uniting payments and technology and igniting new relationships, with an extensive complement of six conference tracks, 59 educational sessions, and an exhibit floor that will take attendee engagement to new levels.

New Exhibit Hall Features

TRANSACT remains at the payments forefront by affording more than 200 companies an unprecedented chance to demonstrate their latest products and services, encourage and share ideas, provide inspiration, and connect with other payments professionals. And with many new additions this year, the 55,000-square-foot trade show floor is a must-visit destination for all attendees.

Topping the list of exhibit hall highlights is the Retail Technology Zone. This area promises to generate significant buzz among attendees given the accelerating rate of change and innovation within retail technology, coupled with the convergence of payments and point of sale, which can lead to new opportunities for all industry stakeholders—from hardware manufacturers and application software providers to processors and resellers.

With that in mind, the Retail Technology Zone will showcase the latest solutions for connecting hardware and software at the point of sale, with an extensive array of traditional fixed and mobile solutions to be featured. These solutions will enable retailers to take advantage of new value-added services, in turn maximizing their potential to grow their businesses by easily adapting to changing demands around all aspects of the customer experience.

Among the vendors participating in the Retail Technology Zone will be several first-time exhibitors, including Zebra Technologies. Todd Virgil, global OEM (original equipment manufacturer) leader, says he and his colleagues look forward to the opportunity to demonstrate to retailers, merchants, independent software vendors, OEMs, and payment entities how Zebra's retail solutions help to reduce costs, improve associate effectiveness, and increase shopper satisfaction.

Along with other initiatives, such as the formation of a Retail Tech Committee, the inclusion of the Retail Technology Zone on the trade show floor is part of a larger initiative by ETA to engage the retail technology industry. To that end, complementing the pavilion will be an exclusive educational forum, "Retail Solutions 2.0—The Future of Value Added Selling." Designed as a deep dive into how retailers can adapt to changes in the market and evolving consumer behaviors and take advantage of

new value-added services that make integration possible through technology, the forum will cover the impact of mobile devices on retail, pain points for merchants, and the impact of EMV. Sponsored by Sage Payment Solutions, the sessions will encompass:

How Mobile Devices Are Changing Retail Commerce. This session will cover the growth in mobile device shipments, new opportunities and challenges, and value-added services that make integration possible. Speakers are Marc Castrechini, ETA CPP, vice president, product management, Cayan, and Rich Aberman, co-founder, WePay. Rick Oglesby, senior analyst/consultant, Double Diamond Payments Research, will moderate.

Merchants and Payments: The Top Five Issues and Opportunities. Panelists will explore the issue of whether retailers can make Big Data, mobile commerce, EMV, customer authentication, and technology work for them, or if these issues will merely consume time and resources. Moderated by Mark Horwedel, CEO, Merchant Advisory Group, panelists include Ken Grogan, manager, treasury services, Wakefern Food Corp.; Jamie Henry, senior director, emerging payments, Walmart Stores Inc.; and Maureen Elworthy, director, treasury, Ahold.

Fireside Chats. Mike Cook, senior vice president and assistant treasurer of Walmart Stores Inc., and ETA CEO Jason Oxman will discuss how Walmart, the world's largest merchant, evaluates consumer payment acceptance, including emerging payments. They also will explore how the retailer is changing the payments landscape and responding quickly to new consumer behaviors to save shoppers time and money.

POS + Payments = Business Opportunities. This panel, moderated by consultant Joe Finizio, will feature a look at the business opportunities provided by the convergence of the POS retail technology and payment industries. Ideas for moving forward with, as well as benefitting and profiting from, these opportunities will be provided. Speakers include Henry Helgeson, ETA CPP, CEO and founder, Cayan; Jeff Riley, CEO, Dinerware; John Badovinac, head of integrated payments, Discover Financial Services; and Jason Richelson, founder and CEO, ShopKeep POS.

Also making its debut this year—and certain to generate excitement in light of the growing acceptance of cryptocurrencies by merchants—is the World of Bitcoin exhibit showcase. Here, digital currency providers will highlight their new products and services as they connect with payments industry leaders. By exploring the booths within this centerpiece of the exhibit floor, TRANSACT 15 attendees will quickly garner an understanding of the value of offering Bitcoin to merchants and the benefits

to be reaped by merchants that accept cryptocurrencies.

The addition of World of Bitcoin to TRANSACT 15 dovetails with a recently established partnership between ETA and BitPay, a World of Bitcoin exhibitor and Bitcoin payment processor. Under the partnership umbrella, ETA has become the first trade association to accept Bitcoin payments for trade show exhibition and sponsorship, association membership, and professional development programs.

The World of Bitcoin comprises part of the Payments Next Zone, a major attraction of the show. Within an easy-to-navigate area of the exhibit floor, the Payments Next Zone will serve as a one-stop shop for an extensive array of cutting-edge technologies and vendors—everything from startups to Big Data and digital currencies companies and other groundbreaking advances from across the payments landscape.

Yet another newcomer to the exhibit floor lineup is an interactive "commerce experience" offered by Intel at its booth. In the largest exhibit space in TRANSACT history, at 2,500 square feet, Intel and its partners will share insights into the future of transactions and the retail industry, with an emphasis on how consumers derive value from the Internet of Things (IoT). Industry stakeholders also will learn how Intel's solutions play an important role in sharpening retailers' competitive edge and connecting payments professionals to new opportunities. Intel currently provides an extensive portfolio of open and scalable solutions that enable application developers, among them payments application developers, to connect, protect, and manage "things" with pre-validated building blocks.

"Intel is pleased to exhibit at TRANSACT 15 and to demonstrate current and future secured payment technologies that are pertinent to the ever-growing Internet of Things," says Doug Davis, senior vice president and general manager of Intel's IoT Group. "Intel is committed to delivering scalable, end-to-end hardware and software payment and security solutions, and we look forward to interactive discussion with attendees on options to secure payments."

Whether you're just getting your feet wet in the retail and payments profession, or you are a seasoned veteran, attending TRANSACT 15 and exploring these new features of the trade show floor—as well as attending the wealth of other educational sessions and events—is a move you'll definitely want to make. ***TT***

TRANSACTION TRENDS EXCLUSIVE CE SERIES

Breach Response for the Small Merchant

Follow these nine guidelines to add value to your merchant relationship

When Home Depot suffered a data security breach last year, hackers made off with 56 million payment card details. Understandably, the breadth of the incident garnered nationwide media attention: If every cardholder were a U.S. citizen, nearly one sixth of the population was affected.

While large retailers are the ones in the spotlight for breaches, small merchants, by far, are the most common targets of thieves, according to the ETA whitepaper, *Data Breach Response: A Nine-Step Guide for Smaller Merchants*. And when such breaches do occur, ISOs and acquirers can play an important role by counseling their merchant customers through what is likely a fear-inspiring and intimidating process.

Remember, prompt action is crucial when fraud is suspected, and the merchant's risks grow exponentially when a data breach is ignored. The following nine guidelines are intended for ISOs, acquirers, and payments facilitators to use when helping their merchant clients create a data-breach response plan, which is a PCI Security Standards requirement.

1. Don't cut power. A merchant's first instinct in the event of a breach might be to power down its payment network or change passwords. While it is important to assist merchants in quickly stopping a breach, it also is important to instruct them to preserve evidence, as much as possible, which can help to determine how their system was compromised. While there should be consideration to isolating the part of the merchant's system that has been compromised, the merchant should not power down its system or alter log-in information. That can destroy critical data, which investigators might need in the aftermath of the breach. Merchants should contact their processor or a PCI investigator.

2. Identify a lead person. Some businesses are so small that the only person capable of leading the response effort is the owner him- or herself. If the business is larger, help leaders identify the employee to whom all information about the breach and strategies for next steps are directed.

Earn ETA CPP Continuing Education Credits

Throughout 2015, *Transaction Trends* will provide readers with executive summaries of ETA whitepapers and industry thought leadership. Read this article, then visit www.electran.org/cpp for a link to the quiz to test your knowledge and earn 2 ETA CPP CE credits per quiz!

3. Retain privacy counsel with experience in data breach response. A merchant that suffers a data breach needs to comply with both federal and state laws. Most states require that breach victims notify individuals whose information is in danger of being at risk. (In many areas of payments law, the state of California is at the forefront of the latest requirements. Having familiarity with California law could be useful for any merchant as a possible guideline. However, it is important to stress that each merchant that falls victim to a breach must comply with the state laws in the jurisdiction governing the merchant.) As a result, it is important for merchants to retain privacy counsel with specific experience in data breach notification. If the merchant carries insurance, the insurer may provide a list of law firms from which the merchant can choose.

Once a merchant retains privacy counsel, the counsel will advise on which potentially affected consumers, government agencies, law enforcement, and other third parties to notify of the breach.

4. Notify the insurer (or insurance broker). Cyber insurance is growing increasingly common. In the case of Home Depot, a third-quarter 2014 filing with the U.S. Securities and Exchange Commission indicated that the company spent $43 million on investigations, providing identity theft protection services to consumers and increased call center staffing, along with other legal and professional services. However, more than one third of that cost—$15 million—was covered by an insurance policy. It is important to note that the failure to inform an insurer promptly can limit or undermine possible reimbursement.

5. Work with the processor. A notification from its processor may be the merchant's first sign of a potential breach. Explain to the merchant that the processor shares the same goal of minimizing liability exposure associated with breaches and they should work together. If the merchant does not have a back-up payments system in place, the processor should work with the merchant to create one and get the merchant's payment system back up and running quickly, even as a potential investigation continues. While it might be an unpleasant fact that a processor has to hold back some funds to address potential liability, work carefully with the merchant to explain why these actions must take place. Remind the merchant that the processor is its best advocate for reducing potential exposure and minimizing risk.

6. Retain a PCI Forensic Investigator (PFI). Often, the card brands will insist that a merchant retain a PFI to investigate a potential breach and ensure it has been contained. This can be done directly for a merchant or through its legal counsel. On its website, the PCI Security Standards Council has a list of PCI Certified Forensic Investigators and explains how its "program establishes and maintains rules and requirements regarding eligibility, selection, and performance of companies that provide forensic investigation services to ensure they meet PCI Security Standards. The PFI program aims to help simplify and expedite procedures for approving and engaging forensic investigators." The program accomplishes this by providing a single set of requirements for investigators and also by providing guidance on how investigations are to be conducted and reported.

7. Take remedial action. Encourage the merchant to work with its processor and the PFI to take the recommended steps to ensure the breach has been stopped and any vulnerabilities are fixed.

8. Create a communications plan. A merchant, in conjunction with its legal counsel, will have to communicate the extent of the breach to both internal and external stakeholders. If you have experience with successful communications strategies in this regard, you may want to pass along to your merchant client what has worked in the past.

The January 2014 Target breach response is one example. CEO Gregg Steinhafel took a multipronged approach, which included an appearance on CNBC and an open apology letter to customers that detailed Target's responses.

While small businesses will not have the same access to large, national media organizations, they may, however, reach out to local media and other outside parties with accurate and reassuring messages to customers and other stakeholders.

9. Document and preserve records. Merchants need to document each step of their response—including breach identification, investigation, and remediation—and carefully preserve their records. If maintained correctly, these records can help the merchant ensure appropriate actions are being taken and minimize legal liability or regulatory investigations by the FTC, individual state attorneys general, and other authorities in the future. Helping the merchant with these efforts can strengthen your business relationship for years to come.

The information provided here is a summary of the whitepaper *Data Breach Response: A Nine-Step Guide for Smaller Merchants*, written by the ETA's Risk, Fraud, and Security Committee in collaboration with Arnall Golden Gregory LLP. ETA members can log in and download the full whitepaper for free at http://bit.ly/1C4oiid. The information is intended to provide general information regarding issues related to data breach response. It does not provide legal advice. Although our writers have gone to great lengths to make sure the information is accurate and useful, it is recommended that merchants consult with their lawyer for legal advice. ***TT***

NorthAmerican® BANCARD

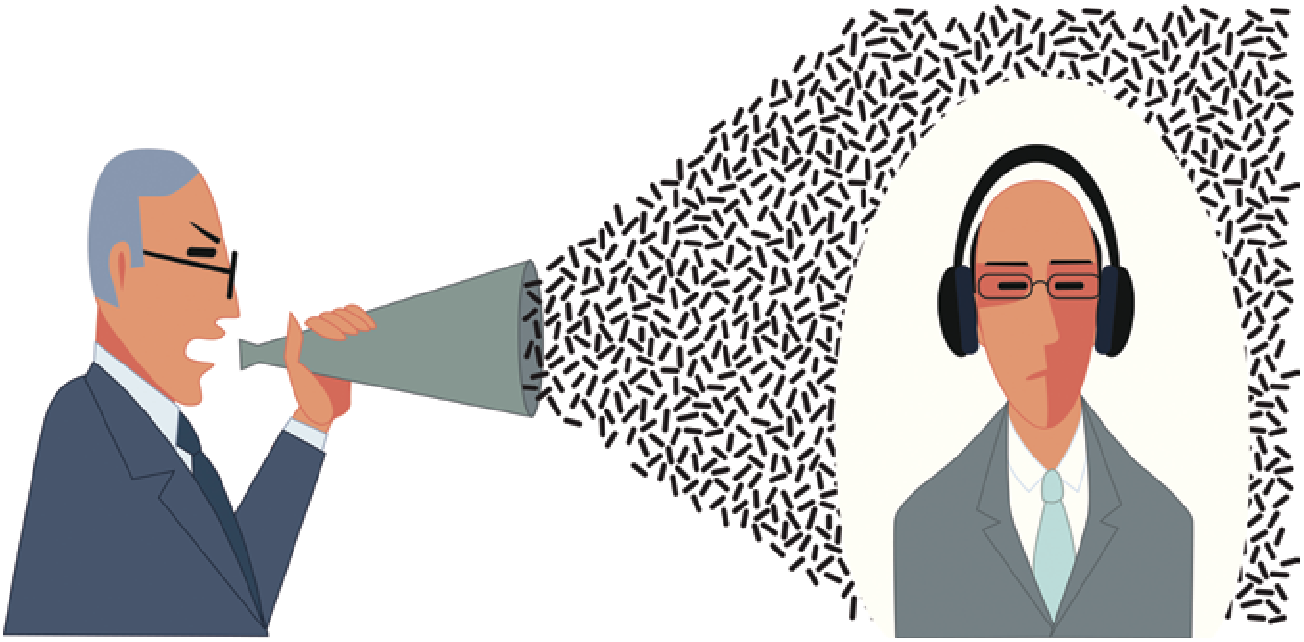
BECAUSE YOU DIDN'T INVEST IN THE PET ROCK.

We're here to help. Think of this as ***your*** Pet Rock. With a wide range of product offerings for any merchant, you can take the leash off and run free. Join North American Bancard, the industry leader, and see just how loyal we are to increasing your bottom line.

2014 ETA AWARDS
ISO OF THE YEAR

VISIT US AT TRANSACT15 - BOOTH 735

1.877.447.2256 | GONAB.COM/ROCK



Why Aren't You Listening to Me?

Real examples of and remedies for communication breakdowns between processors and ISOs

Communication between processors, ISOs, and other industry constituents—as well as internal communication within each type of organization—is a sensitive topic in the payments sector. Stakeholders question why their partners are not listening to them and go so far as to complain about it. But in many cases, the disconnect remains, and unpleasant consequences ensue.

Processor Perspective

Processors believe a lack of understanding about the ramifications of failing to close the communications gap, the absence of defined internal responsibilities for handling issues, or other catalysts cause ISOs to slough off warnings about potential problems. Consider this real-life example: In the course of regular monitoring, a processor discovered fraudsters were using an ISO's merchant processing credentials to test whether certain card numbers could be used for nefarious purposes. The processor contacted the ISO about the activity. It also reminded the ISO that edits, which were readily available, would stop the testing activity but were not being used.

The fraudulent exercise continued, however, despite the fact that the processor contacted the ISO daily to point out the problem. On the fourth day of activity, the ISO took action by activating available edits, and only then did the fraudulent activity stop. But major damage had already been done: The perpetrators were able to execute more than 100,000 fraudulent authorization at-

Meet the Experts

The best practices and examples highlighted in this column were contributed by:

Kathy Baker, **ETA CPP**, director, risk and compliance, enterprise business compliances, TSYS Acquiring Solutions

Rhonda Lemos, senior vice president, risk management, Merchants Choice Payment Solutions

Jennifer Maddux, senior program manager, risk process excellence, Intuit Inc.

Lance S. Rich Jr., director, risk management, ProPay, A TSYS Company tempts on numerous credit cards.

The processor observed that had the ISO taken action on the first day—immediately after learning about the situation—the fraudsters would have been able to test far fewer credit cards (25,000 in one day, as opposed to 100,000 in four days). Even more importantly, the ISO would not have been responsible for the authorization fees that covered the 100,000 authorization attempts.

Whether inadvertently or because of organizational breakdown, ISOs also have been known to allow some communications from processors and other payment industry partners—issuers among them—to fall through the cracks. Consider a different ISO's story, which unfolded as it was conducting an investigation of major international counterfeit card transactions. The ISO was confused about the transaction behavior. An indication that the card involved was chip-and-PIN enabled caused concern, because the ISO did not support chip-and-PIN transactions.The ISO also had a question about a specific POS entry mode.

An employee of the ISO reached out to MasterCard for guidance and feedback. Upon hearing an explanation of the situation, the MasterCard representative inquired whether the ISO had seen, reviewed, and taken action on a MasterCard Security Notice that had been distributed in October of the previous year. The ISO employee conceded that the organization had not been aware of the vulnerability notice and had not read the bulletin. The latter, the MasterCard representative explained, had provided specific, simple instructions for adjusting authorization parameters to decline any transaction that met the criteria outlined in the notice (and fit the description of the peculiarities the ISO had encountered). The result of this slip-up: a $30,000 loss tied to counterfeit transactions. Occurrences such as this also lead to cardholder inconvenience and a lack of confidence among senior management that the proper controls are in place and loss goals can be met.

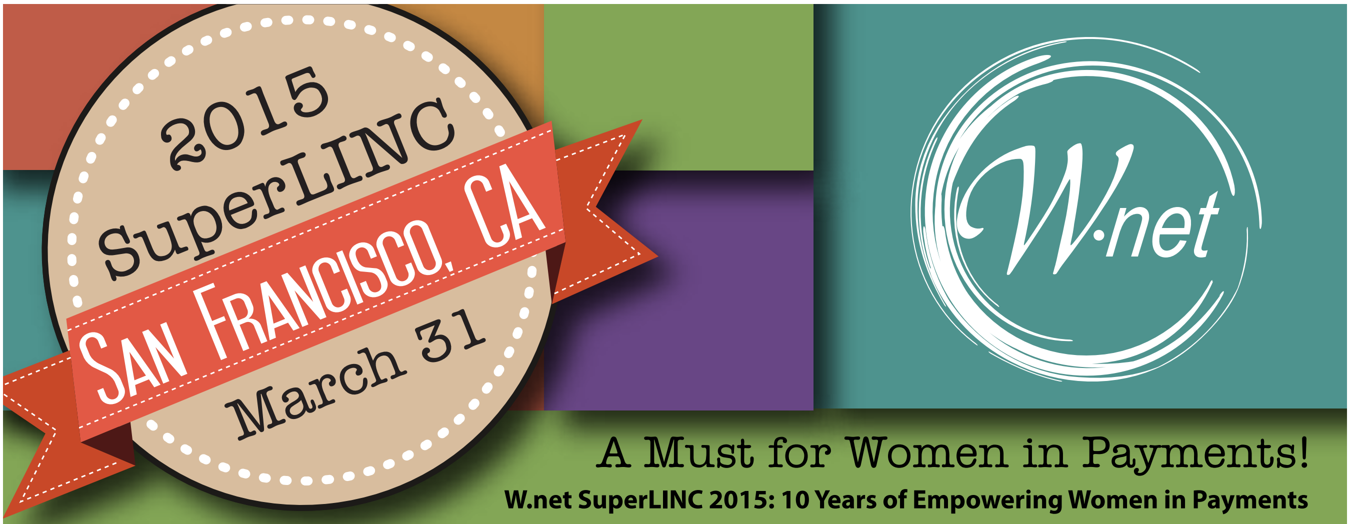
The ISO Perspective

Meanwhile, ISOs say processors sometimes are slow to address issues that are brought to their attention, "pass the buck" when it comes to solving problems, or offer only limited solutions when situations are brought to their attention. In another non hypothetical situation, an ISO began to receive complaints from customers regarding inflated month-end authorization fees. Fees that normally totaled about $40 per customer suddenly added up to thousands of dollars per customer.

A review by the ISO revealed that the authorization and settlement setup on all of the affected accounts was identical. At the same time, the ISO was hit with a flurry of notifications from issuers regarding suspicious activity originating at its merchants' locations. Several of these issuers confirmed that they had identified a common authorization point.

Upon notifying the authorizing entity, the ISO learned that this was a common scenario, and there were some system settings that would alleviate the issue. The authorizing entity also recommended that the ISO conduct a portfolio review prior to modifying the settings.

Despite adhering to the authorizing entity's advice, the ISO continued to receive complaints from merchants as it attempted to address the problem. Suspicious activity, too, was ongoing. The issue was escalated to senior staff of the authorizing entity, and



the ISO finally was given the assistance it needed to quickly remedy the situation.

While the ISO's difficulties were eventually eliminated, the additional cost associated with the snafus cut into revenue. More importantly, the organization sacrificed some of its credibility and probably lost customers.

Changing the Course

There are simple ways to make it easier for ISOs and processors to listen to each other. Notably, regular communications channels and protocols should replace a more casual approach to disseminating information. Protocols should apply to communication between ISOs and processors, as well as to communication among constituents at each type of organization. The latter should include opening communications channels so that information flows upstream and downstream. ISOs would do well to set up periodic phone or webinar information-sharing sessions with agents.

Another true anecdote proves the value of regular communications between ISO and processor partners: A processor and ISO have established a practice of conducting monthly calls to review accounts, problems, identified issues, and the like. Recently, during such a call, the two entities reviewed the monthly statistics of accounts that had been submitted to MATCH for underwriting and determined that account submissions for the last half of the month seemed to have dropped off.

This was a trigger point for the ISO to review its file submission procedures. The review revealed an error in the reporting mechanism, which was easily remedied. However, had the review not helped pinpoint the error and led to rapid remediation, the possibility of on-boarding known bad actors would have remained unchecked.

Moreover, establishing internal and external accountability within ISO and processor organizations is critical. For example, on the ISO side, specific individuals should be responsible for ensuring that information received from processors (and other entities) has been shared with the correct parties—and that it is acted upon. On the processor side, individuals should be accountable for acknowledging the receipt of communications from ISOs and going beyond giving them vague or generic suggestions for handling problems, which forces ISOs to escalate issues for remediation.

Additionally, policies should call for designated parties to ensure that suggested or agreed-upon actions have really been taken. This includes following up on email communications, which ISOs and processors both admit can get lost in the ether.

Finally, ISOs and processors agree that departments other than risk management should be involved in devising solutions to problems—whether these problems concern ISOs and processors themselves or merchant clients. These departments include IT, customer care, and finance.

It is unlikely that ISOs and processors will always experience a perfect level of communication. Nonetheless, recognizing what can happen when poor communication and only sporadic listening are the norm, and following best practices to support a new normal, will go a long way toward minimizing risk and improving relationships. ***TT***

ADVERTISERS INDEX

Company	Page	Phone	Web
Apriva	20	480-421-1275	www.apriva.com
Authorize.Net	1	425-586-6000	www.authorize.net
Discover Network US	6-7	800-347-2000	www.discovernetwork.com
eProcessing Network	13	805-551-7411	www.eprocessingnetwork.com
EVO Payments Intl.	9	800-227-3794	www.EVOpayments.com
FIME America	11	+1 408 228 4040	www.fime.com
Magtek, Inc.	C2	562-546-6603	www.magtek.com
National Merchant Association	5	866-509-7199	www.ProAgentPartner.com
North American Bancard	35	877-447-2256	
Nuspay International, Inc.	27		www.nuspay.com
Pax Technology	2		
PAY.ON America Inc.	17	914-954-4891	www.payon.com
Paytrace	C3		www.paytrace.com
Planet Group Inc.	21	800-9799166	www.planetgroupinc.com
Star Micronics	19	800-782-7632	www.starmicronics.com
Total Merchant Services	C4	877-498-2807	www.totalpartnership.com
USA ePay	30	866-812-3729	www.usaepay.com
Women's Network in Electronic Transactions (W.net)	37	877-772-WNET	www.wnetoline.org

Brian Sadowski

As CIO of Apriva, a provider of secure end-to-end wireless transaction and information solutions, Brian Sadowski keeps a finger on the pulse of data security. *Transaction Trends* sat down with Sadowski to identify the most pressing concerns and how the industry should be addressing them.

What data security issues are you currently seeing in your work?

With the proliferation of fraudulent activities over the past 12 to 18 months, there is a need to look for vulnerabilities in every nook and cranny where data—personally identifiable information (PII) and cardholder information—reside. Keeping up with these vulnerabilities, which change as fraudsters become more sophisticated and the volume of data for the taking continues to grow, is in itself an enormous challenge.

In the past, securing data at rest within databases and files was sufficient. Now, this isn't enough, because so much data is moving across the landscape. Fraudsters today are not only getting into databases that house data at rest; they're also attempting to infiltrate any system that holds data in transit throughout the payment system.

Keeping up with and addressing vulnerabilities inherent in widely used protocols is a major issue as well. The Padding Oracle On Downgraded Legacy Encryption (POODLE) vulnerability, which affects the Secure Socket Layer (SSL) is a prime example. *[Editor's note: Considered high risk under the umbrella of the Payment Card Industry Data Security Standard (PCI DSS), POODLE is a vulnerability of the SSLv3 protocol. Exploiting POODLE in the context of a payment gateway or any other business model where cardholder data is transmitted over SSL can expose cardholder data.]*

We believe the PCI SSC will probably announce that the SSL is no longer an approved protocol for transaction processing. There will be limited time for organizations to remediate or modify applications to remain PCI compliant.

Where are the biggest problems?

Everywhere. The single biggest problem is that the way we address data security today isn't necessarily going to work tomorrow, because targets and schemes constantly change.

How should these issues be addressed?

There are no ubiquitous solutions; there has to be a combination of solutions and a security strategy that calls for looking for vulnerabilities everywhere and proactively addressing them.

Data security must be approached from the inside out. Organizations need to implement solutions that are purpose-built for security—not bolt-on solutions. One kind of solution isn't sufficient—it's not just tokenization, or encryption, or another technology alone. It's a combination.

It's also important for organizations to avoid the temptation to create their own data security solutions. They're bound to miss some part of the moving threat target. The development of threats will outpace the development of solutions.

What's the catalyst for today's breaches?

The overall move online is a key factor here. Merchants have moved away from—and continue to move away from—dial-up terminals, replacing them with IP-based equipment. Dial-up terminals are secure because they are purpose-built, but when transactions are processed via the Internet as with IP-based systems, data are exposed to public areas. It's like begging for commercial hackers to attack.

What's more, the trend toward Big Data means a much greater volume of data and activity information is out there for perpetrators to access and sell for nefarious purposes. The proliferation of business intelligence apps and products that collect and provide consumer-level data adds fuel to the fire. The more data you have, the better the chance of misappropriation and misuse.

Is this just the tip of the iceberg?

We're neither at a point where we can say that the worst is over, nor at the high point of the tip.

EMV has long been regarded by some parties as an all-encompassing panacea for data security ills, and that's a mistake. We can look to other regions where EMV is now the norm, and clearly see how it can help with data security, but it's obvious that it still isn't enough. A combination of EMV, tokenization, and encryption is needed in order for there to be meaningful impact in repelling attacks. And even when all of those are in place, something else is coming.

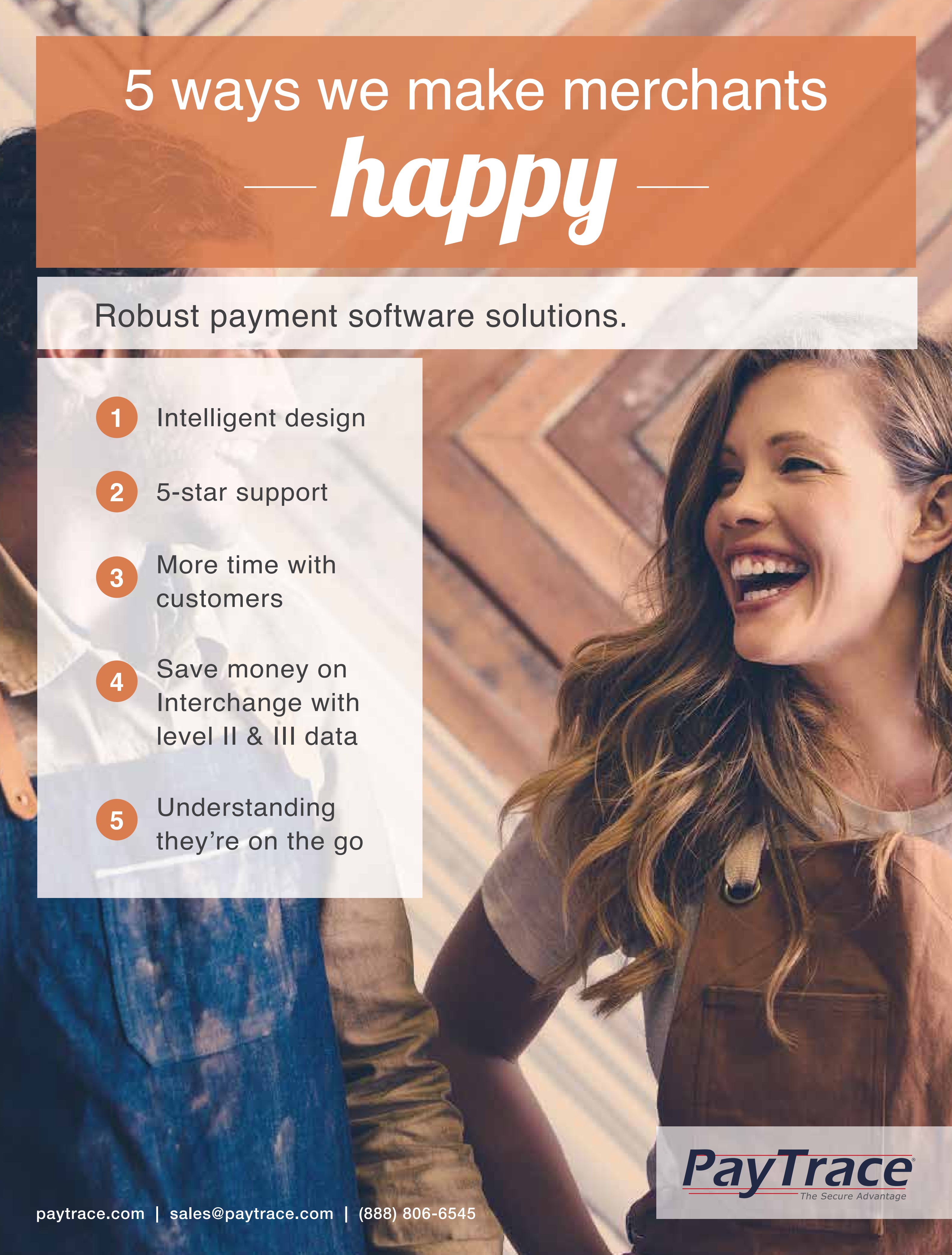
What role should ISOs play in data security at the merchant level?

ISOs and MSPs need to go beyond selling solutions. It's incumbent on them to assist merchants in achieving and maintaining a high level of data security.

Tier 4 merchants, in particular, need help here. They don't know what "secure" means, and they don't entirely comprehend that the cost of a single data breach may be enough to drive them out of business. They haven't been hackers' biggest target, because there has been more for the taking from larger merchants.

However, this will eventually change as Tiers 1, 2, and even Tier 3 move ahead with new security issues. ISOs should be pushing all clients to do the small things, such as changing passwords regularly, and the more significant things, like migrating to an EMV platform, to ensure their survival going forward. ***TT***

—Julie Ritzer Ross



5 ways we make merchants — *happy* —

Robust payment software solutions.

1. Intelligent design
2. 5-star support
3. More time with customers
4. Save money on Interchange with level II & III data
5. Understanding they're on the go

PayTrace®
The Secure Advantage

paytrace.com | sales@paytrace.com | (888) 806-6545

ingenico
MasterCard
VISA
Please present card
Amount: $28.95
iWL250
CreditCard
1234 5678 1234 5678
CARDHOLDER NAME
Done