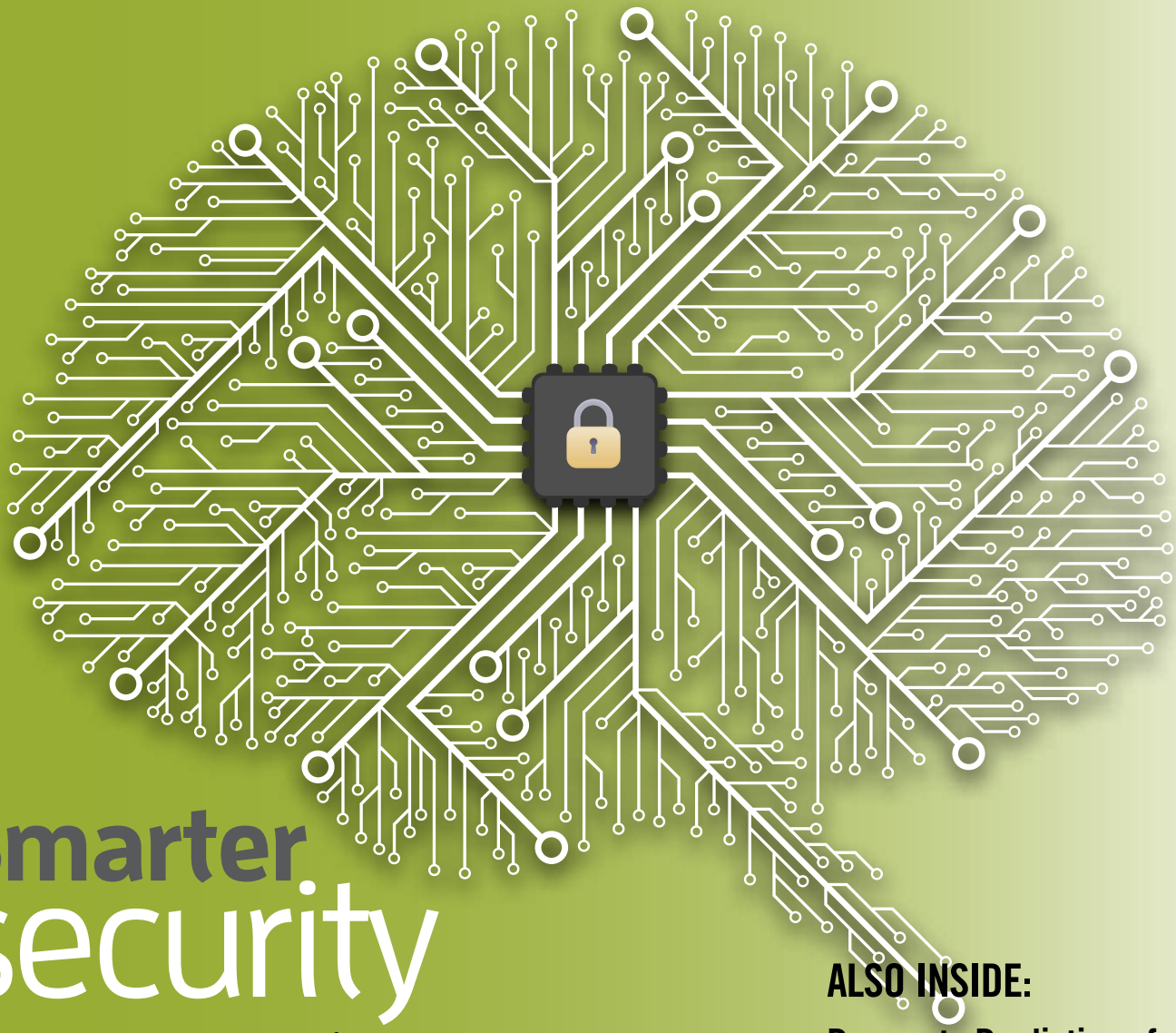
Exclusive: New Guidelines for Underwriting and Risk Monitoring **PAGE 16**

January/February 2016

TRANSACTION trends

ETA
THE OFFICIAL PUBLICATION OF THE
ELECTRONIC TRANSACTIONS ASSOCIATION



Smarter security

Data protection reaches new levels of sophistication

ALSO INSIDE:

Secure Payments Confidently

With strong encryption and industry proven card authentication inside the reader head, cards and sensitive cardholder data are protected at the very first point of interaction with a MagneSafe™ enabled payment device.

If that's not enough, the data is also dynamically tokenized with every transaction, whether the consumer pays with a secure swipe, a chip, or a mobile phone.

Trust the industry experts to help you fully secure your payment environment.

DynaPro*

- EMV Compliant & Certified
- MagnePrint® Authentication
- P2PE Validated KIF
- NFC-Enabled*

DynaPro Mini**

- Tokenization
- 3DES Encryption
- Bluetooth Mobile**
- Certified to Multiple POS Platforms

FIND OUT MORE 562.546.6467 sales@magtek.com www.magtek.com

contents

The Official Publication of the Electronic Transactions Association Vol. 21 | No. 1

features

departments

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
Jeff Mankoff, Ed McKinley, Julie Ritzer Ross, Josephine Rossi, and Amy Zirkle

Advertising Sales
Alison Bashian
Advertising Sales Manager
Phone: 703/964.1240 ext. 28
Fax: 703/964.1246
abashian@conferencemanagers.com

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.**

@ETA

Defining Payments

We all know that 2016 will be truly transformative for the payments industry. Our expanded payments ecosystem encompasses more players than ever, as traditional payments players expand into new business segments while the world's largest technology companies launch innovative new payments services and seek partners in our industry. The rate of payments technology adoption is remarkable: It took nearly 15 years for 25 percent of U.S. businesses to adopt electronic card processing—but by the end of this year, only two years after Apple Pay's debut, we will see 25 percent of merchants accepting mobile payments.

Our critical, but previously somewhat invisible, industry is now in the headlines as consumers use their new EMV cards, explore mobile payments options, seek out more personalized shopping experiences, and demand the best in security for their transactions.

As payments technology steps into the spotlight, ETA steps up to the plate. We are the trade association of the entire payments industry, with a unique vantage point on our industry's transformation. With more than 500 member companies, including the biggest payments and technology companies in the world, ETA is driving this industry evolution.

Not surprisingly, many new events and organizations are trying to capitalize on the growth in payments and innovation in our industry. But only ETA—the non profit trade association of the payments industry—has a mission to grow our members' business. ETA gives our growing member base the keys to unlock success in today's transformative payments space. We have expanded our focus to embrace important new players and to empower legacy leaders through increased member benefits and the biggest ever event in payments: TRANSACT. By investing in education, research, advocacy, and events, ETA invests in our industry. At TRANSACT 16, the global stage for payments innovation, our industry will get business done. (Read more about the TRANSACT 16 agenda on page 19.)

Join us as we define the future of payments at TRANSACT 16!

Jason Oxman
Chief Executive Officer
Electronic Transactions Association

"HOW I TURNED A $450 INVESTMENT INTO $48 MILLION!"

Eric Bostic
ETA CPP

Getting the ETA CPP credential was the game-changer for Eric Bostic's career.

When the CFO of a $48 million account had to choose an agent, Eric's ETA CPP became the deciding factor. His credential not only gave him added confidence, it represented knowledge and a level of integrity his client found reassuring. See how adding six letters to your name can be your smartest investment.

*Take the next step in your career. Visit **electran.org/etacpp** today to get started.*

Only the *CERTIFIED* will *THRIVE!*

ETA CPP™ CERTIFIED PAYMENTS PROFESSIONAL

IT Pros See Rise in Security Risks to Payments Data

A new study has found escalating security risks to payments data and a lack of confidence in securing mobile payments methods among global IT professionals. The study shows a critical need for organizations to improve their payments data security practices.

More than half of the 3,700 IT professionals surveyed said their companies had suffered a data breach involving payments data, four times in the past two years on average, according to the report, "Global Study on the State of Payment Security." The study, which was conducted by the Ponemon Institute on behalf of Gemalto, surveyed IT security practitioners from major industry sectors.

In one finding, 55 percent of respondents did not know where all of their payments data is stored or located. In addition, ownership for payments data security is not centralized, with 28 percent of respondents saying responsibility is with the CIO, 26 percent saying it is with the business unit, 19 percent with the compliance department, 15 percent with the chief information security officer, and 14 percent with other departments.

Also troubling is the finding that payments data security is not a top five security priority for their company, according to more than half of respondents. Less than one third (31 percent) feel their company allocates enough resources to protecting payments data. Nearly three quarters said their companies are either not PCI DSS compliant or are only partially compliant.

"The payment landscape is evolving. As we move toward online and mobile payments, it's clear that we are entering a new era of payment data protection," says Jack Jania, senior vice president of strategic alliances at Gemalto. "That is made especially apparent by the 54 percent of survey respondents who stated that payment data security is not a top five security priority for their company. There is a definite need for a change in mindset, including an understanding of where payment data is stored and how security can apply to 'data at rest' and 'data in motion.' The fact that only 44 percent of businesses use encryption or other end-to-end crypto tools to protect payment data from the point of sale to when it is sent to a financial institution or stored needs to be addressed."

The study also examined respondents' use of new payments methods, finding that respondents expect use of mobile, contactless, and e-wallet payments methods to double in the next 24 months. Mobile payments are predicted to account for 18 percent of all payments in two years, up from just 9 percent today.

Companies are likely to face even more difficulties in securing new payments methods. In fact, the study found that nearly three quarters (72 percent) believe new payments methods are putting payments data at risk, and 54 percent do not believe or are unsure that their organization's existing security protocols are capable of supporting these platforms.

Fast Fact

Wrongly rejecting a good customer is a costly mistake for merchants, as **66 percent of consumers who experienced a false decline** limited or entirely stopped their patronage of the declining merchant.

Source: "How Consumers Respond to False Positive Declines," conducted by Javelin on behalf of Riskified

Report Forecasts Growth in EMV and Contactless Acceptance

In 2015, issuance of cards adhering to the Europay, MasterCard, and Visa (EMV) standard in the United States exceeded original industry expectations, hitting nearly 600 million units. The U.S. and China led significant worldwide market growth, accounting for 53 percent of the more than 2.6 billion total EMV cards shipped in 2015, according to ABI Research.

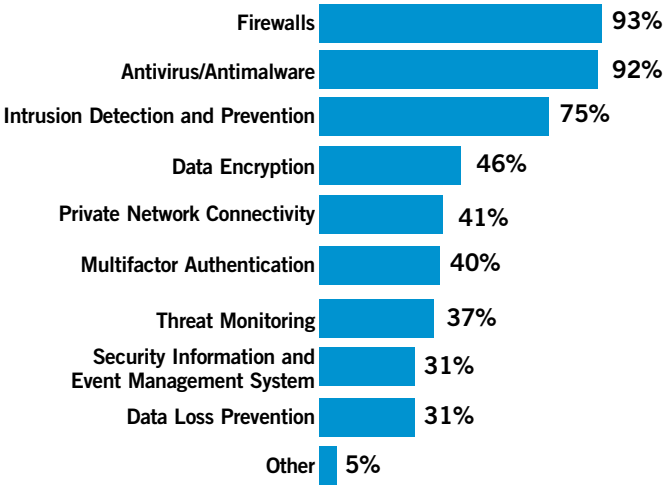
"EMV migration in the U.S. ramped up quickly, with market penetration likely to hit close to 100 percent over the next two years," says Phil Sealy, senior analyst at ABI Research. However, a U.S. market dip is expected within the next two years: "Our findings show that U.S. EMV shipments will peak in 2016 and reach approximately 617 million units. In 2017, shipments are forecast to dip by approximately 5 percent, with later shipments likely to settle within the 600 and 615 million range," says Sealy.

Additional opportunities in the U.S. are presenting themselves due to the market's large installed base of mag-stripe private label credit cards (PLCCs) and next-generation migration plans surrounding contactless issuance, according to the ABI Research analysts. U.S. PLCC migration may provide a growth boost from a volume perspective. However, the major vendors are expressing great interest in local issuers' plans around contactless migration. A move to contactless may present a substantial value proposition for leading smart card players.

"In 2015, Apple and Samsung Pay helped educate U.S issuers and users on the value and convenience that contactless payments can enable," says Sealy. "In the longer term, this will help drive uptake of contactless cards. However, ABI Research believes that the U.S. will remain primarily a contact-based country for the short term. The country will most likely issue contactless cards upon expiration of the contact cards. We anticipate a larger contactless card impact in the U.S. and worldwide to be felt in two to three years' time."

Infographic

Top Security Technologies Used To Protect Payments Data



Source: "Global Study on the State of Payment Security," conducted by the Ponemon Institute on behalf of Gemalto

Note: More than one response permitted

Moves & Mergers

Prepaid card services provider **Blackhawk Network Holdings Inc.** has acquired **GiftCards.com LLC** and **OmniCard LLC** for $120 million. GiftCards.com specializes in selling digital and physical prepaid cards through its website. OmniCard sells customized prepaid incentive and rewards cards to businesses.

First American Payment Systems has purchased the entire portfolio of ISO accounts and associated contracts from **Chase Commerce Solutions,** the global payment processing and merchant acquiring business of **JPMorgan Chase & Co.**

Ingenico Group has announced the creation of The Ingenico Group Unattended Partner Program to help accelerate EMV and NFC payment acceptance in unattended environments. Inaugural partners include Creditcall, Flex, FreedomPay, IBM Commercial Services, Image Manufacturing Group, INTOUCH, KIOSK Information Systems, Livewire Digital, Nanonation, Olea Kiosks Inc., Scan Source, Tempus Technologies, TrustCommerce, Unattended Card Payments, and Zivelo.

TSYS has entered into a definitive agreement with Vista Equity Partners to acquire **TransFirst,** a Vista portfolio company, in an all-cash transaction valued at approximately $2.35 billion. As a result of the transaction, TSYS reportedly will be the sixth largest U.S acquirer based on net revenue, supporting more than 645,000 merchant outlets.

Verifone has signed an agreement to acquire **AJB Software Design Inc.,** a Toronto-based provider of payment gateway and switching solutions for large merchants in the United States and Canada.

Payments Predictions

Look to these five areas for growth in 2016

By Amy Zirkle

When the *New York Times* recently ran an article on its front page about Sweden emerging as a future cashless society, we knew payments was really starting to garner attention from the broader world—outside those of us who live and breathe this stuff on a regular basis. Mind you, ETA doesn't presume that the next big Oscar contender will be a movie about payments exclusively (well, we are coming up on Oscar time). But, the *Times* article does mean that the recognition of electronic payments and moving away from cash is significant—and hey, it was on the front page.

Even with electronic payments becoming more commonplace, there is much to consider about what this year will mean for payments and, in particular, the technology that will further guide development and support of a host of new offerings. Here's a look at some of the most notable, high-level areas of growth:

Mobile payments will continue to flourish. Mobile payments will, no doubt, continue to assert itself as the mode of choice for payments. As more and more service providers develop payment applications for utilization of mobile devices for in-store purchases, the portability of payments offered by mobile devices and services will surge. In fact, 2016 could prove to be a big year for those offerings, as well as expanding use by additional verticals.

ETA's Mobile Payments Council will be touching on a number of issues relevant to expanding the growth and acceptance of mobile wallets and mobile payment solutions. In addition, the opportunities that mobile products and services will present to the sales channel should not be overlooked. ETA's newly formed Payment Sales and Strategy Committee will be considering all that mobile will support in terms of service delivery and development of new products.

EMV is here to stay. The fight for data security and consumer protection had a banner day on Oct. 1, 2015, when the Europay/MasterCard/Visa (EMV) standard—or "chip cards"—became the new standard in the United States. Currently, 60 percent of U.S. cardholders have received EMV cards from their banks/card issuers, and it is projected that 44 percent of merchants will be EMV-ready by the end of the year.

Within ETA, all of our subject matter councils and committees are touching upon the wide range of issues resulting from the EMV migration, and developing guidance and additional education tools to address its impact. That guidance will include work from the ETA Risk, Fraud, & Security Council, which will consider matters related to addressing instances of chargebacks and fallback among other issues. Meanwhile, the ETA Retail Technology Committee will be working to further support and guide merchant education, with a targeted focus on small merchants. Moreover, ETA has also created a cross-council committee dedicated solely to EMV industry issues and will likely be developing documents throughout 2016 to provide better understanding of what the impact of the new standard is for the card-not-present (CNP) space.

Biometrics will become more sophisticated. As chip cards wipe out card-present counterfeit fraud, industry experts anticipate an increase in online fraud (also known as CNP fraud). Counterfeit card fraud in the United States is projected to fall more than 50 percent to $1.77 billion between 2015 and 2018, while CNP fraud will jump $3.3 billion to $6.4 billion, an increase of 106 percent. Multifactor identification methods—such as real-time facial recognition and biometric social data mining—are the future of payments. Socure, an industry leader in identity verification solutions, just introduced Perceive, its patented real-time facial biometrics product that instantly matches media profile data, and has the potential to end the need for passwords. Perceive works with the click of a front-facing camera on any smartphone, instantly proving who you are by recognizing facial features.

Without question, the use of biometrics and measures for enhanced authentication will prove increasingly important for the payments ecosystem. Last year, ETA joined as a founding partner with the FIDO (Fast Identity Online) Alliance, in its Cooperation and Liaison program. The goal of that program is to offer relevant perspectives to influence development of FIDO standards to ensure universal strong authentication. ETA will be furthering this partnership in 2016 through work that addresses payments authentication and develops materials to support and expedite the use of robust means for authentication.

Analytics—big and small—enhance value. Much of last year was focused on the role of Big Data and the impact it had on payments. Big Data enables merchants to bring back personalized service by offering greater insight into customer preferences and utilizing digital footprints to support those efforts. Indeed, it is technology that enables merchants to gather the data from its customer base, and prioritize and customize product and service offerings.

But small data can be just as mighty and valuable—and perhaps better serve the payments space. When we think of small data, we consider far more manageable data sets that can be customized with specific attributes to address and consider a designated action, process, or function. As integration continues in payments, the use of small data can offer greater value and help to define a niche service offering.

In 2016, ETA's Technology Council will be continuing its work on the analytics that play a pivotal role for payments. The council will be doing a deeper dive on the role of small data and furthering its discussion about what truly constitutes small data across verticals and how players in the payments ecosystem can access and utilize these analytics to guide product development and enhance customer service and interaction.

The Internet of Things will facilitate relationships. The growth of the Internet of Things (IoT) will necessitate the need for partnerships, alliances, and relationships with payment companies. Samsung and MasterCard announced a new service called "Groceries by MasterCard," which will enable consumers to order groceries directly from their Samsung Family Hub Smart Refrigerators. As IoT expands, there is no limit to the opportunities it presents for commerce and the direct benefits it can offer the payment industry.

In 2016, ETA will conduct a number of projects to look at what IoT will facilitate for the payments ecosystem. No doubt the devices, advancements, and technologies that make all of these breakthroughs possible are offering the payments industry new possibilities and relationships once never thought possible.

Here's to an exciting year ahead! ***TT***

Amy Zirkle is director of industry affairs for ETA. Reach her at azirkle@electran.org.

By Ed McKinley

Rise of the Machines

As big banks and payments pros add AI to their IT systems, use cases emerge for security, merchant monitoring, and more

For generations of movie fans, the phrase "artificial intelligence" brings to mind the computer HAL 9000's unblinking red eye and chillingly calm voice in the film *2001: A Space Odyssey*. Others might think of actor Haley Joel Osment's portrayal of the robot child capable of love in the movie *A.I.* But yesterday's science fiction can become today's science, and the term "AI" is now entering the vocabulary of the payments business.

Still, opinions vary on what exactly AI means. For Rich L. Stuppy, chief operating officer of Kount, a fraud and risk-management vendor, AI came into being during the middle of the 20th century, when computers began following orders. But the public's definition of AI, he says, became a moving target, redefined as whatever lies just beyond the current state of computer technology. Julie Conroy, research director for Aite Group's retail banking practice, offers a different interpretation: "It's when you have computer technology that's able to learn on the fly from new inputs without having to go back and be retrained. 'Unsupervised model' is one of the buzz words."

Todd Clark, senior vice president for First Data Corp. and head of the STAR Network and Debit Processing Group, provides a helpful analogy: It's as broad and vague as saying "automobile" instead of "1957 Chevy Bel Air." In his last job, Clark served as senior vice president of worldwide sales for Feedzai, an AI vendor. He's more comfortable discussing the specific idea of "machine learning" than the larger concept of AI. Machine learning's underlying algorithms make it quicker to train, quicker to learn, and more able to handle a high volume of work than other forms of AI, he says.

Matthew Parker, cofounder of a vendor called KYC SiteScan, agrees that it's preferable to focus discussion on machine learning instead of trying to pin down the vague notion of AI. "We have a lot of discussions internally about AI," he says of the semantics involved. "It's a layman's term. From a technical point of view, it doesn't exist."

Payments professionals often prefer to think of AI as machine learning or automated decision-making. By those definitions, it's already becoming a force in the industry's perennial struggle to maintain a technical advantage over data thieves. That's important because "when the merchant is either unwilling or unable to honor that chargeback, we stand in the shoes of the merchant and make that cardholder whole," notes Geoffrey Stocki, vice president of operations for acquirer and transaction processor North American Bancard.

AI can also foil bogus merchants. "The business case hinges on the need to understand your merchants' behaviors," Conroy says. "Is this merchant real, and is he really selling what he says he is?" Some industry players regard AI as the power behind the Know Your Customer (KYC) and Anti-Money Laundering (AML) processes. Both acronyms carry a "compliance connotation," and, as Conroy explains, they're becoming increasingly important to acquirers as concern about regulation intensifies.

Profit From the Statistics

Whichever term suits—the broad AI or the precise machine learning—the discussion soon proceeds beyond programming based on simple instructions, according to Sandeep Grover, senior vice president of global e-commerce at Feedzai. He says it's not just telling a computer that "if" a certain thing happens, it should "then" perform a specified task. To explain the complexity, Grover suggests thinking of self-driving cars.

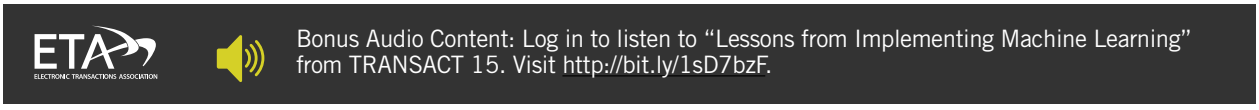
Simply writing rules for a computer produces a few overly generic categories that cannot begin to take into account the vast number of cases that can become part of the model that results from the observations of machine learning, Grover continues. When changes occur in the market, machine learning adjusts immediately, as opposed to human-driven reaction that can take a long time, he maintains.

However one chooses to understand AI, the technology lived on the "bleeding edge" just a few years ago and now constitutes the "wave of the future," according to Clark. Setting up or modifying AI takes days instead of weeks or months, he says, and its workings are measured in milliseconds.

> "THE BUSINESS CASE HINGES ON THE NEED TO UNDERSTAND YOUR MERCHANTS' BEHAVIORS. IS THIS MERCHANT REAL, AND IS HE REALLY SELLING WHAT HE SAYS HE IS?"
>
> —JULIE CONROY, AITE GROUP

At First Data, the number of use cases for machine learning appears endless. It's useful anywhere the company has a lot of data. And AI makes the data practical because it shows the reasons for rejecting a particular file instead of merely saying it's rejected, he notes.

The company is using machine learning for merchant underwriting, Clark says. Instead of underwriting merchants when they sign on and then checking on them again once a year, machine learning allows the company to track every transaction. The security division also is using machine learning to assess companywide threats



to its own systems, he says.

First Data often comes up in industry discussions of AI or machine learning prowess, but the company's not alone at the forefront. Late last year, North American Bancard began testing a machine-learning tool that the company refers to as a custom risk-scoring model, says Stocki. He considers the system so "cutting edge" and such a great "competitive advantage" that he declines to name the vendor working on it.

The system monitors transactions and builds a statistical record of the ones that result in chargebacks, he says. By learning what characteristics indicate risk, the system becomes better at detecting potential problems, Stocki says. "Over time, the system refines the model," he maintains.

If, for example, someone is making $200 purchases in a coffee shop at 11 p.m., that merchant might be selling something other than coffee, he notes. In another example of suspicious behavior, a thief might repeatedly make significant purchases in a short time with the same card, indicating a merchant or customer is using stolen card information.

"MACHINE LEARNING ALLOWS US TO LOOK FOR ANOMALIES AND PATTERNS THAT ARE DOWN TO A FIELD OF ONE. THE RESULTS ARE EXTREMELY PROMISING."

—TODD CLARK, FIRST DATA CORP.

The relief isn't limited to the acquiring business. The STAR Network began using AI to monitor transactions internally last summer and started sharing the results with customers in January, Clark says. It can push all of its volume through, not just a subset of it. "It's kind of like that '95 Impala and a Tesla," he notes, continuing the automotive analogy. "Both cars—but very different."

The STAR Network doesn't view AI from a KYC or AML perspective because all it has to work with is a card number, not the cardholder's name or other information, Clark explains. So the company bases decisions on how and where the cardholder used the card in the past. "We're using Feedzai's engines to develop a profile of that card," he says.

Until now, a company might have tracked American Express transactions, documenting, for example, that green card customers spend $300 a month and sometimes make late payments, gold card users spend $2,000 a month and pay on time, and platinum card shoppers spend $5,000 a month, Clark explains. "With machine learning, we're able to take it down to an individual card level," and know what constitutes usual behavior with a single card. That means if a customer who generally doesn't shop on weekdays and doesn't buy clothes walks into a Gap and buys $400 worth of jeans, something's possibly amiss.

That granular detail isn't possible with a rules-based approach because it would require humans to write so many rules. With machine learning, however, that level of detail becomes possible. "You don't have to have a thousand people sitting in a room poring over data," Clark observes. "Machine learning allows us to look for anomalies and patterns that are down to a field of one." The results are extremely promising, he says of what the company is achieving with AI. However, good results require a basis of good data, he asserts.

Consumers Cognition

It's also important to note, Clark insists, that machine learning can improve the customer experience by reducing the number of valid transactions that are rejected. Vitally, it can do that without slowing down the process, he asserts. "If we continue down this path, STAR will have the highest approval rate and the lowest fraud rate in the industry," he says. "That's our stated goal."

Elsewhere, North American Bancard finds other uses for the technology that's arguably akin to AI. It helps automate the work of evaluating, bringing onboard, and monitoring merchants. In the past, employees spent time researching prospective clients with computer searches, street maps, Yellow Pages listings, Better Business Bureau complaints, and government records of pending actions, says Stocki. Now, software from KYC SiteScan scans records automatically and produces a document with its findings, Stocki says. His company has added that capability to the automated, customized underwriting workflow process created with another vendor, ContractPal Inc. It entails writing rules that direct the program to notify humans when particular situations arise.

"If we get a hit on the CFPB [Consumer Financial Protection Bureau] site, for example, it kicks it out for an underwriter to review instead of sending it on to the next step," Stocki says. "So, we're spending our underwriters' time only where there's a problem that needs review." When problems don't arise, a less-skilled employee can handle the application without the help of a more-qualified underwriter, he says. Some applications receive approval without review by a credit analyst because they meet all of the criteria, Stocki explains. "We're able to give credit decisions in minutes instead of hours or days."

Matching what's on the application with what's available in public records has reduced the number of cases where criminals succeed in stealing a merchant's identity "tremendously," according to Stocki. Although it's hard to quantify, he suggests automation has reduced the number of fraudulent accounts boarded by at least 10 percent.

Automated onboarding has improved the customer experience by decreasing waiting time for merchants that don't require extensive review. For example, at nail salons, where the services have been rendered, chargebacks seldom occur, there's no forward delivery, and the cardholder is present for the transaction, Stocki says. "They can be processing with us the very next day," he notes.

Watchful Eyes

About 60 percent of merchant applications that acquirers process with KYC SiteScan meet the automated standards and don't require human review, says Parker. Acquirers shouldn't reject applications without having a human set of eyes on the file, he suggests. The human touch remains vital, agrees Clark. "Sometimes they do end up in the hands of humans," Clark says of cases that call for decisions. "This is not a matter of turning the machines loose to figure it all out."

The system flags possible problems but doesn't get the final say. "It doesn't remove the human element," Stocki says. "The fear is that the machines are going to take over, but there's no substitute for human judgment." The system merely flags inconsistencies for humans to review, he says. People judge the relevance of an anomaly and consider the circumstances surrounding it.

"If you had enough horsepower, you could probably program a machine to go through the variations of it, but, at this point in time, [the systems] aren't ready for that," Stocki says.

Even if they fall short of taking total responsibility for security, such systems could do a lot to keep merchants ahead of criminals bent on finding the newest ways to crack computer systems to steal card data, Stocki says. "We can save ourselves a lot of heartache," he observes.

By using AI to enhance security and avoid those heartaches, professionals in the payments industry believe such exemplary behavior could make state and federal regulators look upon them more favorably. Scrutiny by agencies like the Federal Trade Commission and the CFPB is forcing acquirers to maintain 24-7 vigilance, according to Barry Sloane, president, chairman, and CEO of Newtek Business Services Corp. The federal government's Operation Choke Point accused a Newtek subsidiary of wrongdoing in processing payments for a client engaged in illegal telemarketing schemes. The Feds obtained a monetary judgment against Newtek in federal court, but Sloane says the company has filed an appeal.

Sloane advocates combining technology like AI with human-powered diligence to avoid problems: "It would be great to have a solution where you run everything through a computer model, and it does everything for you. Unfortunately, the world doesn't work that way."

Regulation makes news, but Stocki claims he doesn't lose sleep over it because his company is campaigning to prevent losses to consumers and merchants. As he says, "If you're doing the right thing, you should have nothing to fear." ***TT***

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

Security Movement

By Julie Ritzer Ross

TECHNOLOGICAL AND ORGANIZATIONAL CHANGE COLOR DATA SECURITY TRENDS, SAY RESEARCHER AND CONSULTANTS

The old adage that the more things change, the more they stay the same, may apply somewhere in the electronic payments space, but not when it comes to data security. Change is everywhere as perpetrators find more data sources to infiltrate, and organizations scurry to implement new technology to mitigate their risk.

"New threats continue to emerge because criminals are clever and continually innovate," Avivah Litan, vice president and distinguished analyst, Gartner Research, tells *Transaction Trends*. Once they hone in on a vulnerability, these lawbreakers will escalate their attacks as victimized entities scramble to plug security holes.

Vikas Bhatia, CEO, Kalki Consulting, agrees, adding that "it's not just growth in the number of threats that is marked; expansion in the type of information being breached is making news."

Litan, Bhatia, and other experts say that although many trends are currently shaping the status of data security, some are more notable than others. Here's a look at what's top of mind for analysts and researchers this year.

1 Encryption and tokenization are front and center. The upgrade of POS systems to comply with the Europay/MasterCard/Visa (EMV) standard and accommodate chip card-enabled transactions as prescribed by the EMV liability shift, which went into effect this past October, is moving along. As of Oct. 30, 2015, the Payments Security Task Force pegged the volume of merchants that had migrated to EMV-compliant POS equipment at 25 percent and predicted that number would double by the end of that year.

While updated statistics were not available at press time, Litan says that as fraudsters shift their attention to the small to medium-size businesses (SMBs) that have not upgraded to EMV-compliant POS hardware, those merchants will capitulate and board the EMV adoption train. In Gartner's blog, Litan writes, "if the U.S. is anything like Europe—which it is—the major gain for EMV is for the banks, (which) will see a reduction in counterfeit fraud that they are normally liable for. At the same time, retailers will see an increase in [card-not-present] CNP e-commerce fraud."

But EMV compliance is only one part of the essen-

tial payment security ammunition triangle. The other two sides are made up of end-to-end encryption, also known as point-to-point (P2P) encryption (or P2PE), and tokenization. P2P encryption has evolved into the merchants' "next line of defense" in the battle for data security, according to Boston Retail Partners. The consulting firm's "2015 POS/Customer Engagement Benchmarking Survey" reveals a 151 percent increase in the use of end-to-end encryption by year-end 2016. Of retailers participating in the survey, 35 percent have already deployed end-to-end encryption technology, while 45 percent said they had intended to do so by October 2015, and 8 percent after October 2015. Only 12 percent had no plans to jump on the end-to-end encryption bandwagon

Lori Breitzke, president, E&S Consulting and vertical marketing manager, North America, VeriFone, notes that much of the heightened appeal of P2PE is because it secures and encrypts data from the merchant network and POS systems on a hardware "end" to hardware "end" basis, rather than on a software "point" to software "point" basis. Although the latter can be effective, she explains that it leaves an entrée for malware to infiltrate merchants' systems.

A component of the PCI Security Standards Council's (PCI SSC) P2PE Program also is helping to spur P2PE acceptance. Under the program umbrella, P2PE technology vendors have the option to validate their P2PE solutions and applications. Merchants that install a PCI SSC-validated P2PE solution intended to work in tandem with technology that complies with the EMV standard have the advantages of increased security from hardware-to-hardware encryption and a reduction in the scope of their PCI Data Security Standard (DSS) assessments. To qualify for validation, a given P2PE solution must comply with the PCI SSC P2PE Standard. As such, it encrypts cardholder data from the point at which a payment card is accepted by a POS device after it has been swiped through or dipped into a magnetic stripe reader to the point at which the third-party processor or acquirer decrypts the data for processing. "That's a pretty big deal for them," Breitzke observes.

As for tokenization, Boston Retail Partners' research projects a 145 percent boost in the use of tokenization solutions before the close of 2016. One-third (33 percent) of merchants polled for the study had already rolled out such technology when the research was conducted last year. An additional 40 percent cited plans to have it in place by October of 2015, and 8 percent after that date. Again, only a small portion of respondents (19 percent) had no intention of pursuing tokenization as a payment security avenue.

Breitzke believes tokenization has rapidly gained ground in part because by making data impervious to decryption (and hence, being deciphered) except with a special key, it removes merchants from the scope of the PCI DSS and protects data from compromise in the physical and remote (cyber) channels alike. However, the fact that "tokens are formatted in a manner similar to that used to format card information"—in turn eliminating the need to make major changes in payment acceptance systems—"comes into play here as well," says Breitzke.

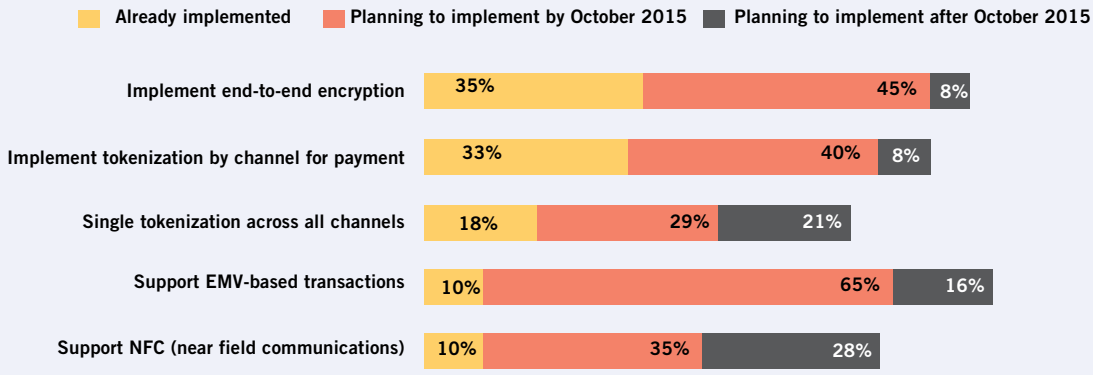
Interestingly, some observers also foresee that encryption increasingly will be used for nefarious purposes. Litan cites as an example "more use of encryption by cybercriminals, cyber-spies, and other disaffected parties" to prevent law enforcement officials from gaining insight into their activities. Lawbreakers can decrypt any data they have generated that pertains to their criminal activities. That encryption will be such that even officials with decryption software and "back doors" into hardware operating systems and encryption/decryption software won't be able to make sense of it.

2 **POS systems are experiencing more malware attacks.** The most recent "Data Breach Investigations Report" issued by Verizon and Trustwave indicates that on average, merchants across 61 nations were hit with a collective 800-plus malware attacks weekly in 2015. These attacks are becoming increasingly sophisticated, the report reveals, with about 70 percent involving a combination of techniques to infiltrate merchants' POS systems. Just as significantly, of 79,790 security incidents investigated by Verizon for the report, more than one-quarter of data breaches (28.5 percent) are attributable to attacks on POS systems.

Of particular note on the POS-attacking malware front is modular POS (ModPOS), according to cybersecurity firm iSight. ModPOS utilizes a complex, sophisticated code base that permits it to evade detection. Its modular nature allows it to pursue multiple attack routes, with keylogger, POS scraper, and upload/download modules that permit it to hone in on unique aspects of merchants' POS systems. According to an iSight report, one ModPOS module has been observed grabbing credit-card track data from the memory components of POS systems. This, the report states, indicates "possible targeting of any sector that uses POS systems, including retail, foodservice, hospitality, and health care."

iSight claims that even retailers whose POS systems have been upgraded in keeping with the EMV liability

Payment Security Technology Plans



Source: "2015 POS/Customer Engagement Survey," Boston Retail Partners

shift cannot be considered immune to ModPOS and similar malware. The reason: If the POS system has not been configured to support end-to-end encryption and encrypted data in memory, ModPOS and other malware that uses RAM scraping techniques can still yield fraudsters access to payment card data. The latter may then be employed to complete online purchases that do not require physical card presence.

ModPOS is "the most sophisticated POS malware we have seen to date," writes Stephen Ward, iSight's marketing manager, on his company's blog. "In a nutshell, this is not your daddy's run-of-the-mill cybercrime malware."

3 **The Internet of Things introduces new vulnerabilities.** The connection of devices to each other via the Internet—i.e., the Internet of Things (IoT)—is starting to create vulnerabilities within the payment system, with little relief in sight given projections of its growth. By Gartner's estimates, 6.4 billion connected "things" (i.e., devices) will be in use globally by year-end, up 30 percent from 2015. The technology research firm forecasts that figure will reach 20.8 billion by the year 2020.

"The idea of IoT-connected wearable devices, including those with biometric security capabilities" and from payment-enabled watches to clothing and jewelry, is appealing to consumers for the sake of convenience alone, says Chris Bucolo, senior manager, partner relations, for professional consulting firm Sikich LLP. However, Bucolo, who specializes in payment technology, points out that despite such attraction, potential problems remain. Case in point: still-shaky authentication and authorization, as well as insecure software and firmware. All leave data more vulnerable to hacking open doors wide for data vulnerability and headaches in the short term.

"The small size and limited processing power of many connected devices could inhibit encryption and other robust security measures," Edith Ramirez, U.S. Federal Trade Commission chairwoman, noted in an address at the Consumer Electronics Show in January 2015. "Moreover, some connected devices are low-cost and essentially disposable. If vulnerability is discovered on that type of device, it may be difficult to update the software or apply a patch—or even get news of a fix to consumers."

4 **Threats to personally identifiable information are on the upswing.** As hackers continue their attempts to steal payment data—and focus on small merchants that have yet to implement EMV-compliant point-of-sale technology as well as on those whose CNP business removes EMV from the data protection equation—they are increasingly turning their attention to personally identifiable information (PII). PII is defined as an individual's first or last name, combined with a Social Security number, driver's license or state-issued ID card number, and any account number (credit, debit, membership, etc.) and associated security code, PIN, or password. The smartest thieves realize that unauthorized access to such information is easier to gain than access to payment data because the former is not subject to the PCI DSS—and, according to Litan, is not typically encrypted. At the same time, these theives are figuring out how to employ stolen PII to exploit payment systems and products.

Litan predicts that "criminals will be busy exploiting the vast amounts of PII and identity intelligence that have

been stolen over the past few years and subsequently purchased to commit identity fraud."

Just as significant, merchants' vulnerability to PII theft is increasing as loyalty programs and similar marketing initiatives boost the volume of data about individual consumers they collect and generate, according to Marion H. Roger, vice president, Hospitality Evolution Resources, a hotel management and technology consulting firm. Hotels rank at the top of the list of merchant categories in which susceptibility to PII data compromise is becoming prevalent, Roger notes. She attributes that trend to the fact that lodging establishments often collect and retain certain information retailers, for instance, do not (e.g., driver's license numbers).

However, restaurant operators and health care providers—the latter, based on the routine practice of recording patients' Social Security numbers—are falling victim to the phenomenon as well. Roger points to an incident that occurred at Starbucks as an example of PII compromise: In mid-2015, news broke that fraudsters had hacked the coffee chain's app and siphoned money out of users' gift card accounts. The thieves accessed the app and carried out their scheme by first obtaining cardholders' passwords and usernames, then adding a new gift card for each and transferring funds from victims' cards onto fraudulent gift cards. That enabled them to steal all the money on users' apps.

Chris Zoladz, founder and principal of security consulting firm Navigate LLC, reports that in addition to introducing administrative measures and bolstering physical security by further restricting access to physical servers, a growing number of merchants are harnessing new encryption and tokenization technologies to stem the PII compromise tide. One such solution is the Personally Identifiable Information Tokenization process from payment processor and technology services provider CardConnect, which encodes individual pieces of information (e.g., names, Social Security numbers, and program membership numbers) and stores them as irreversible tokens. If a data breach occurs, hackers are unable to access anything other than strings of characters that lack a relationship to the sensitive information. PCI XML Inbound is another option. Offered by PCI Booking, this solution is designed specifically for hotels; it allows PII and payment data to be imported into hotels' property management systems in encrypted format rather than in plain-text format.

In another vein, entities like Elavon are striking integration deals aimed at giving PII security a boost. Elavon recently signed a multi year agreement with Wyndham Hotel Group under whose terms EMV and tokenization were incorporated into the hotelier's property management system via Elavon's Fusebox payment gateway and Simplify payment security software application.

Moreover, Roger and Zoladz note, tokenization and encryption solutions are being developed and embraced to protect PII in Big Data analytics conducted using tools like Hadoop. Voltage Secure DataSuite from HP Security Voltage makes such a tool. It combines tokenization and format-preserving encryption, thereby permitting plain text of a specified format to be encrypted into a ciphertext of identical format. Encryption reportedly is simplified because there is no need to alter intermediate systems and data storage layouts to get the job done.

Predictive analysis takes hold. Organizations, including Tier 1 and Tier 2 merchants, are increasingly adopting a "sophisticated" approach to cybersecurity that no longer is limited to "locking the doors after the robbery has been committed," according to "Analytics Trends 2016: The New Frontier," a report by consulting and professional services firm Deloitte. The report states that these entities are beginning to leverage more predictive approaches to threat intelligence and monitoring—"in short, going on the offensive." In addition to scrutinizing Internet chatter, this may entail engaging cyber-professionals for the purpose of monitoring previous hacks to forecast which threats are likely to surface next.

"In many" instances, Deloitte experts write, taking advantage of predictive analysis also means systematic and continuous probing of internal defenses "to make sure others don't find a security hole first." They also advocate taking advantage of analytics to detect patterns of internal (i.e., employee) and external behavior that may indicate not only that a compromise or other threat to data security has occurred, but that one (or more) is about to occur.

Such players, the report stipulates, will also be seeking out experts with new capabilities, as many third-party cyber-professionals lack the skill to conduct predictive threat intelligence or predictive analysis of past breaches. "At the very least, extensive collaboration between analytics and cyber-professionals may be required," the report concludes.

Clearly, data security has come quite a ways over the past few years, when EMV, P2PE, and tokenization were not yet a reality in the United States. But it is equally obvious that new threats continue to surface, and that new means of addressing them will need to be implemented in the near- and long-term. ***TT***

Julie Ritzer Ross is a contributing writer for Transaction Trends.

Full Exposure, Part 2

Updates to the seminal guidelines benchmark risk assessment and liability mitigation

In 2014, an ETA working group developed the "Guidelines on Merchant and ISO Underwriting and Risk Monitoring" to help the payments community prevent undesirable merchants from entering or remaining in the card acceptance ecosystem. The guidelines serve as industry best practices and have become vital to ensuring the most rigorous efforts around underwriting and risk monitoring for merchants and ISOs.

Since the guidelines' debut, the payments industry has endured significant change, and this month ETA's Risk, Fraud, and Security Council has released an updated version to keep pace with that fast-moving evolution. The new guidelines represent one of the many tools the industry uses to combat fraud and give policymakers peace of mind that the industry is proactive in protecting consumers and the payments industry. Dozens of ETA member companies participated in the revision process to address topics such as payday lending, debt collection and relief, charitable donation sites, payment aggregators/facilitators, and more.

"As fraudsters build a 10-foot wall, we must build an 11-foot ladder," says Scott Talbott, ETA's senior vice president of government relations. "The revised guidelines are the 11-foot ladder."

Prior to the release, *Transaction Trends* received exclusive access to the new version of the guidelines. Here, we highlight the substantive updates and additions with an overview and explanation of the changes. The following summary is not all-inclusive, and ETA members are strongly encouraged to download and read the complete updated version.

Merchants Requiring Enhanced Underwriting Due Diligence

One of the first sections to be updated clarifies that, aside from merchants engaged in illegal activities and merchant categories prohibited by acquirers, mandating categorical exclusions of merchants based on their industry or business type isn't required. Of course, some higher risk merchants require more diligence and case-by-case assessments of risk. As a result, some of the advice may be unnecessary for a particular merchant relationship, the authors say. Other steps should be augmented by additional measures to protect against reputational risk and injury to consumers, as well as increased risk monitoring during the merchant relationship.

Additional key updates to this section:

Interrelated companies and beneficial owners. According to recent consumer protection law enforcement efforts, merchants continue to set up companies and process accounts to bypass screening and hide the true identities of the persons controlling these companies and accounts. The guidelines now recommend ETA members take additional steps to monitor for attempts to conceal interrelated companies or true owners' identities by obtaining basic corporate information from each

BONUS CONTENT: Log in to **http://bit.ly/1LTaFGr** to download the complete updated guidelines, and visit http://bit.ly/1B1Teer to hear the audio session from TRANSACT 15 that explains how to implement the guidelines in your business.

prospective merchant, as well as any corporate name, trade name, fictitious name, or alias under which such merchant or persons do or have done business. ETA members also should request and cross-check information on related companies, principals, and beneficial owners against those of other merchant accounts. If the merchant has any beneficial owners not listed in the application materials, members should determine if the listed principals and the beneficial owners are related, live in the same area, belong to similar organizations, or are linked on social media sites. The updates recommend members perform searches on customer service, contact, and cell phone numbers.

Certain marketing practices. The authors made several updates to better help ETA members identify the types of marketing and sales practices prone to issues under laws that prohibit unfair, deceptive, or abusive acts or practices. As a result, they added fantasy sports and other small-dollar consumer lending products—including car title loans and money transfers—to the list of example merchant types that may merit attestation.

They also added substantive recommendations for reviewing offer terms and conditions for merchants engaged in negative option marketing, which treats the consumer's silence or failure to act affirmatively as acceptance of an offer. The additions were tracked to match requirements under the Restore Online Shoppers Confidence Act, which has served as a basis for numerous consumer protection actions recently brought by the Federal Trade Commission (FTC).

Enhanced Review of Certain Merchant Types

Eight new subsections were added to provide ETA members with targeted guidance for serving merchants in certain higher risk industries that have been the subject of consumer protection law enforcement actions brought by federal and state regulators. They are:

Short-term, small-dollar consumer lending/payday lending. Payday loans and other small-dollar, short-term loans are prohibited or restricted in some states. ETA members should understand how the lender complies with the laws and any applicable licensing requirements. In addition, the guidelines offer a number of best practices, including requiring the merchant be reviewed by a web scanning service; ensuring the lender takes steps to comply with federal laws and guidelines that apply to its business; and requesting a copy of the lender's state license(s) and lender policies and procedures.

Falsely representing the terms of the loan, repayment, and collection practices is a red flag in the review process. Other tip-offs include failing to clearly and prominently disclose the terms of additional products marketed in connection with the loan (such as prepaid cards or credit insurance) and collecting additional fees and charges not authorized by the loan documents.

Debt collection. ETA members providing services to debt collectors must have a complete understanding of the legal framework under which the merchants may operate and know whether the merchants' practices are permitted under applicable federal and state laws and card brand rules. The new guidelines say legitimate debt collectors are likely to be licensed/registered with the states, record telephone calls to prove lawful collections practices, operate in a manner consistent with consumer protection operations manuals, and appropriately document the debt.

The authors suggest reviewing application information, online complaints, and any other information used in the underwriting process. Be aware of behaviors that signal a debt collector is engaged in practices harmful to consumers, such as: using harassing or abusive tactics to pressure consumers to pay their debts; threatening consumers with arrest imprisonment, wage garnishment, and/or property seizure; using company names to falsely imply law firm affiliations; and "upselling" during the same telephone calls in which debts were collected.

Debt relief services. This category includes merchants—such as debt settlers, debt negotiators, and credit counselors/debt managers—that offer programs or services to renegotiate, settle, or in any way alter the terms of payment or other terms of the debt between the consumer and one or more unsecured creditors or debt collectors. These merchants are subject to federal and state consumer protection laws, including the Telemarketing Sales Rule.

Be wary of companies that insist that they are not involved in "debt relief" practices, but rather provide tools and strategies (usually for an upfront fee) to help consumers manage their debt. These companies may actually provide debt relief. Marketing information given to consumers, as well as customer testimonials and consumer complaints, may help confirm or expose the business as a debt relief company. The authors say reputable credit counseling organizations advise consumers on managing money and debt, help develop budgets, and often offer free education. Credit counselors are likely to be certified and trained in consumer credit issues, including money and debt management and budgeting.

Credit repair. Credit repair companies often prey on vulnerable consumers with poor credit reports by promising to remove negative information, which is not legally possible. Credit repair companies are subject to the Credit Repair Organizations Act, enforced by the FTC, and other federal and state laws that make it illegal to make untruthful statements about what they can do. ETA members should review the merchant's application, website, scripts, marketing materials, online complaint sources, and other resources for marketing claims that over-promise service results.

Money-making opportunities/work-from-home/coaching and mentoring. The authors recommend close examination of merchants that offer pricey products or services to assist consumers in self-help or money-making op-

portunities, such as earning income through a home business, obtaining employment for an upfront fee, learning to develop a successful online affiliate marketing business, or earning money by flipping real estate. Merchants in these categories should be reviewed to ensure their marketing and sales practices do not violate consumer protections laws. In addition to reviewing merchant application and underwriting information, checking telemarketing scripts, refund and cancellation policies, fulfillment materials, in-person seminar programs, product and cost structure, online reputation and complaints, and other sources may help identify questionable practices. The Electronic Retailing Association Self-Regulatory Program Coaching and Mentoring Program is an industry self-regulatory program in which merchants can voluntarily participate for a review of their lead generation, telemarketing, advertising, and other marketing practices.

"Biz opps" and multilevel marketing. Some business opportunities are subject to the FTC's Business Opportunity Rule, including commercial arrangements where a seller solicits a prospective buyer to enter into a new business, the prospective purchaser makes a required payment, and the seller makes certain types of express or implied claims. Multilevel marketing companies that compensate participants based on sales of products may be legitimate. An unlawful pyramid scheme is typically characterized by a payment structure that rewards participants for recruiting other participants into the program, when the recruitment bonuses are not tied to actual retail sales.

To help determine the difference, ETA members should review the company's history and reputation, including whether the company has been sued for deceptive business practices. The authors also recommend reviewing the merchant's program design, marketing and training materials, compensation structure, and possible expenses incurred by consumer participants.

Fraudulent fundraising/charitable donation scams. These businesses often involve for-profit companies that make misrepresentations about charitable donations, including the identity of the solicitor or how the donations will be used.

The terms of service agreements between for-profit fundraisers and charitable organizations also may be unfair or deceptive. For example, the service provider may keep the majority of donations collected for its services and give very little back to the charitable organization, while the consumers believe all or most of their funds will benefit the charity.

ETA members should review the business arrangements of these relationships, consumer complaints, and other information sources to identify these practices. They also should consider whether evidence from underwriting for a nonprofit merchant suggests the entity has been set up to hide unlawful or criminal activity, facilitate money laundering, or move money out of the country.

Payment aggregators/payment facilitators. The authors created this section because the payment facilitator (PF) model could bring unknown higher risk merchants into the payment system without proper review.

The PF should perform screening and underwriting on the submerchant to ensure the merchant is engaged in lawful activity and is compliant with card brand rules and acquirer requirements. The PF model's transparency enables the card brands to identify each transaction in the aggregated merchant account. "Factoring"—which involves processing transactions through a merchant account for an entity not screened for that account, without approval from the association or acquirer—is a prohibited form of payment aggregation. It may violate state or federal laws that prohibit money laundering, especially if the transactions being factored are linked to illegal activities.

Moving Portfolios and Using Nontraditional Partners/Third-Party Agents

The final two new sections added to the guidelines address moving portfolios and using 1099 sales agents and PFs.

When moving merchant portfolios from one processor or acquirer to another, ISOs should review all information discussed in the guidelines along with specific merchant demographics, including the merchant's MID number, open date, MCC, and the counts and amounts of the past 12 months of transactions, refunds, and chargebacks. Reserves or collateral held could be an indication of a high risk merchant in the portfolio.

Any procedures that are subcontracted to a third-party partner or agent should be vetted accordingly. Depending on the use of 1099 agents, ISOs should perform a minimal level of due diligence to ensure their trustworthiness. Similarly, a PF that takes on the role(s) of the ISO needs to adhere to policies and compliance programs, and the ISO should demonstrate its ability to monitor the PF's activities. Otherwise, the ETA member should oversee the PF, which must follow the ETA member credit policy standards and be registered per the card association guidelines. The PF or ISO must demonstrate the ability to monitor its sponsored merchants' transaction, authorization, and chargeback activities. When the PF is part of the funding stream to the sponsored merchants, the PF should demonstrate its ability to report on the reconciliation of the merchants.

Although this summary is not exhaustive, it should put ETA members at all levels of any organization on the path to safely underwriting, monitoring, and managing merchants and ISOs at varying levels of risk exposure. ***TT***

The information provided here is based on "Guidelines on Merchant and ISO Underwriting and Risk Monitoring," developed by a working group consisting of risk professionals and other personnel from various ETA member companies. Readers should refer to legal or other counsel for complete guidance.

All In for TRANSACT 16

View from the House of Blues Foundation Room at the Mandalay Bay. (MGM Resorts International)

Get to Las Vegas in April to access the latest technologies, network with key decision makers, and hear top-rated industry speakers

When you arrive at TRANSACT 16 in Las Vegas this April, you'll be in very good company. More than 4,000 payments professionals are expected to convene at Mandalay Bay for the largest annual gathering of the electronic payments industry. And the timing couldn't be better.

As Henry Helgeson, CEO and founder of Cayan, forecasts, "2016 is going to be a pivotal year for payments." Payments professionals are continuously on the lookout for the latest information on mobile payments, new technologies, security solutions, and digital currencies, and the Electronic Transactions Association's premier event provides the perfect venue for a gathering of the many stakeholders.

"TRANSACT … brings all of those elements together, in a way that you can actually use that information, and take it to battle when you go back to your office, and put it to work for your organization," says Greg Cohen, president of iPayment Inc.

Today's transactions climate is a "renaissance in the payments industry," with a host of innovative products and services that are changing the way transactions are

Fresh off of a multimillion-dollar expansion, the Mandalay Bay Resort and Casino and the Convention Center now boast more than 900,000 square feet of contiguous exhibit space and more than 3,000 redesigned guest rooms and suites. (MGM Resorts International)

completed, says Drew Soinski, executive director/global enterprise accounts for JPMorgan Chase & Co. "There's just so much out there that needs to be absorbed," says Soinski. And there's no better way to absorb it than by attending TRANSACT 16.

Make Blue Chip Connections

Payments professionals describe TRANSACT as a "can't miss" meeting—primarily due to the countless opportunities to interact with key decision makers from all corners of the payments industry. Leaders from across the payments spectrum will take part in this year's meeting—including representatives from the major mobile network operators and equipment manufacturers as well as online service providers, retailers, major processors, and all of the major card brands and venture capital investors.

ETA CPP CERTIFIED PAYMENTS PROFESSIONAL

Celebrate ETA CPPs at TRANSACT 16

This year, ETA will be awarding the association's 1,000th ETA Certified Payments Professional, and will celebrate this milestone with special recognition to certificants during TRANSACT. Those individuals who earned the ETA CPP credential and who are first-time attendees will receive a 60 percent discount off the full registration rate for the meeting.

In addition, ETA CPPs who are first-time attendees will be featured during a walk-in slideshow, recognized from the TRANSACT 16 stage by ETA CEO Jason Oxman, and invited to attend a networking reception in their honor, among other opportunities.

ETA CPPs who are interested in learning more about this opportunity are asked to contact Brenynn Butler at TRANSACTreg@conferencemanagers.com and use the subject: ETA CPP.

"You have the traditional banking group, and then you have the technology that's infiltrating the system now, and what's great about it is, those dots get connected here," says Kevin Jones, president and CEO of Anovia Payments. "It's been very beneficial to the traditional players in that they've been able to introduce new technologies to their partners in distribution channels, while also providing that distribution channel to the new technology players. So, I think it's really the only place that all of those connect."

Industry leaders will take advantage of opportunities to meet with a number of channel partners—from ISOs to payment processors to upstart technology companies. "You get to have meetings with all of the people that matter, and do it in a very efficient manner," says Steven Klebe, business development for Google.

TRANSACT attracts the up-and-comers of the industry: At last year's meeting, 1,400 first-time attendees took part. Those newcomers should be back this year, and many more new faces from game-changing startup companies are expected in Las Vegas. This event, planned by ETA staff, will offer plenty of opportunities to interact with old friends as well as meet and greet the new players. In this environment, you'll learn "more about yourself, your company, your competitors, the landscape, the technologies—everything payments," says Heather Petersen, CEO of National Merchants Association.

Cash In on Intelligence

The agenda at TRANSACT 16 is fully stocked with keynote speakers and a slate of educational sessions that will help you position your company for success as soon as you return from Las Vegas.

Bill Ready will deliver the opening keynote address on Wednesday. Ready, SVP, global head product and engineering for PayPal, will share his insights on the future of payments. "For years, we have been talking about the rise of mobile payments, and today we are starting to see the full potential that mobile can deliver to the commerce and payments industry," says Ready. "At ETA's TRANSACT 16, I look forward to sharing PayPal's perspective on how we as an industry are using mobile to drive innovation, create better experiences online, in store, and in app, but also drive inclusion and democratization across industries and geographies."

Both Paul Galant and David Nelms will deliver speeches during the Thursday keynote session. Nelms, chairman and CEO of Discover, will focus on the future of financial services, and will discuss how changes in technology, consumer behavior, security, the fintech industry, and regulation are affecting payments. "The pace of change is only accelerating in our industry," says Nelms. "We need to understand the factors that are shaping the future, and more important, we need to know what to do now in order to succeed in the years ahead."

Galant has an abundance of expertise to share as CEO of Verifone and a member of the company's board

of directors. Galant previously served as CEO of Citigroup's Enterprise Payments business- and developed innovative digital payments services for Citi's institutional and government clients. His experiences will guide his presentation.

During the educational sessions, attendees will be able to choose from six tracks covering diverse topics such as mobile payments, politics and policy, global payments, security technology, and much more. As in years past, several ETAU courses will be offered, including introductory sessions on electronic processing, operations, and sales, as well as a session focusing on the guidelines for underwriting, transaction monitoring, and portfolio review.

Make Deals With Exhibitors

With more than 200 exhibitors and representatives from 500-plus member companies expected at TRANSACT 16, there will be plenty to see on the 55,000-square-foot trade show floor. High-profile companies such as PayPal, Visa, MasterCard, Verifone, TransFirst, American Express, WorldPay, and hundreds of others will showcase their latest wares, offering opportunities for attendees to access innovative products and services and form new partnerships.

TRANSACT is known for its innovation, "such as mobile payments, mobile wallets, authentication, tokenization—whether it's real-time ACH or Bitcoin," says Will Graylin, global co-general manager, Samsung Pay, and CEO of LoopPay.

Michael Struttmann, senior vice president and general manager, North America, for PowaPOS, says his company has taken part in TRANSACT in the past and has leveraged the event "as a platform to truly launch the company." This year, "we're really looking forward to TRANSACT 16, and the aspects of trying to reach out and get new customers, and also reconnect with some old friends," says Struttmann.

TRANSACT 16's exhibit space will feature several designated areas where participants can focus on targeted payments solutions. In its second year on the trade show floor, the Retail Technology Zone will serve as the perfect meeting spot for those attendees hoping to capitalize on the changes occurring within retail technology. This space will showcase the latest solutions for connecting hardware and software at the point of sale, with both fixed and mobile solutions as well as value-added services. Everyone from hardware manufacturers to application software providers to processors and resellers will want to browse the Retail Technology Zone.

At the popular Payments Next Zone, participants can view cutting-edge technologies offered by a diverse array of companies, from innovative startups to Big Data and digital currency companies. In addition, the Mobile Payments Zone provides attendees the chance to visit with a number of mobile-based businesses in one easy-to-find location. And the Security Tech Zone will facilitate interaction among attendees, buyers, and partners in the payments security sphere.

Tweet, Post, Share, and WIN

Win free team registration

ETA members are invited to enter a contest to win free TRANSACT 16 registrations for up to five employees. All you need to do is print and fill out a sign with your "Brand Transact Profile" information, then post a selfie of yourself and your payments crew with the sign, via either Twitter **@ETATRANSACT** or Facebook **#TRANSACT16**.

Be creative with your theme. Share your selfie and let your customers, investors, partners, and competitors know that you and your company will be highly visible at TRANSACT 16.

Submissions are due on or before April 1 and will be judged by an independent panel of ETA consultants. The most creative and shared selfie will win up to five free registrations. Visit electran.org/events/transact16 for contest details and to download the sign.

Mix Work and Play

TRANSACT 16 will offer many opportunities to build partnerships through networking and extracurricular events. This year's golf tournament will precede the meeting, taking place on Monday, April 18, at the Reflection Bay Golf Club. The Tuesday evening Exhibit Hall Opening Reception will take place from 5 to 7 p.m., and it will be followed by the Visa President's Dinner & ETA Star Awards Gala.

On Wednesday, attendees can enjoy a networking happy hour in the exhibit hall, where first-time attendees and new members will be invited to mingle in a special location on the show floor. ISOs are invited to an ISO reception at the Sage booth.

Those attendees who are still in town Thursday morning are invited to attend a "hangover breakfast," where participants can cement new and old relationships over mimosas and bloody marys.

No matter which events you choose to take part in, it's clear that TRANSACT 16 will offer exposure to all segments of the payments technology world and help prepare you to take advantage of new opportunities in 2016 and beyond. ***TT***

The ISO's Special Realm

Because card-linked loyalty touches the payment terminal, ISOs are the logical sales channel

By Jeff Mankoff

There was a time when ISOs sold magnetic-stripe "loyalty cards," but demand for those loyalty cards appeared to wane. However, that falloff was not the result of reduced demand but rather poor execution: Customers just did not want to carry another loyalty card. Today, loyalty is in increasing demand, and loyalty provider startups are selling loyalty devices and apps directly to small to medium-sized businesses (SMBs), to the exclusion of ISOs. Thus, two questions arise: Why are ISOs no longer in the loyalty game, and is there an opportunity to get back in? While it appears that ISOs have ceded loyalty to the startups, in 2016 card brands, terminal companies, and Software as a Service (SaaS) loyalty providers are bringing to market terminal integrated card-linked loyalty solutions that vastly improve and streamline the customer loyalty experience for merchants and customers alike—and ISOs are the only ones that can sell them.

The terminal is the ISO's special realm. If it touches the terminal/point of sale (going forward we will use "terminal" to reference both), the merchant is calling the ISO. If ISOs want to sell loyalty, loyalty must touch the terminal. It makes perfect sense for loyalty to be tracked at the terminal because shopping is the key metric.

According to Forrester Data's recent "Forrester Wave: Customer Loyalty, Solutions for Midsize Organizations, Q1 2016" report, "Our data shows that improving customer loyalty is likely to be a top marketing priority for 80 percent of decision makers at midsize organizations in the next 12 months. As a result, they seek loyalty solutions that help companies identify and track customers, reward behavior, and drive deeper engagement and relationships." The loyalty market is big, and SMBs will pay for it.

Who Wants to Download a Loyalty App?

The ISOs' execution failure opened the SMB loyalty market to firms like Belly, which does not touch the terminal. Belly's ($99 to $200 a month) product is a separate device that sits next to the terminal, taking up counter space, with the Belly brand standing between the merchant and customer. As with many other loyalty companies, Belly requires the merchant's customer to download the Belly app to redeem the reward. Because these devices do not touch the payment terminal, the loyalty companies do not need ISOs to sell to the merchant. They sell direct.

Notwithstanding the attempts of the loyalty startups, there is still too much friction with existing loyalty offerings. In addition to not wanting to carry another loyalty card, most SMB customers will not go online and enroll, download an app, provide their mobile number every time they shop, or print a reward. Customers are lazy—and rightfully so. Earning points and redeeming rewards should be as easy as simply paying with the credit or debit card already in their wallets.

Terminal Integrated Card-Linked Loyalty

Terminal integrated card-linked loyalty offers both merchants and their customers a

superior, seamless, and easy loyalty execution by tracking loyalty with the payment cards customers already possess. With card-linked loyalty, every time customers shop and pay with their credit or debit card, they automatically earn points and redeem. No longer does a customer have to carry a separate loyalty card, download an app, provide a number with every purchase, or print a reward. The payment terminal, in effect, becomes the loyalty terminal, displacing any third-party device crowding the counter space. Card-linked loyalty becomes part of the payment process—and just happens.

A merchant's loyalty program should be for the merchant's best customers, with the goals of being easy and automatic, and increasing spending and frequency. This means the card-linked loyalty solution must empower the merchant to enroll its own customers, and the loyalty reward must be redeemable only at that merchant's store. To make this happen, the card-linked loyalty program must be integrated into the merchant's payment terminal.

As mentioned above, the merchant must be able to enroll its own customers. The single best place to enroll members is at the merchant's point of sale. Once customers leave the store, getting them to go online to enroll and provide a credit card is almost impossible. But if the card-linked loyalty program is integrated into the terminal, linking the customer's payment card to the merchant's loyalty program becomes as easy as entering a mobile phone number into the terminal, one time. By integrating with the terminal, the SaaS loyalty provider sees the payment card token in real time, and, if the token is not in the loyalty program, the SaaS provider delivers a prompt to the terminal to enroll the customer. Only if the terminal is integrated with the SaaS loyalty program is it possible for the enrollment prompt to occur. But once integrated, enrolling the merchant's customers is easy.

Today, card-linked offers are being embraced by Facebook, Twitter, Microsoft, and credit card issuing banks in a coalition format. (To learn more about card linking, go to www.cardlinx.org). Presently, card-linked offers are not integrated into the terminal, and, as a result, the discount can only be put back on the credit card statement or in another currency (e.g., airline miles). If a merchant wants its own loyalty program (as opposed to a coalition), then the loyalty reward should be the merchant's reward, only redeemable back at the merchant's terminal. Requiring the reward be redeemable back at the merchant drives another visit back to the merchant, which should be the goal of every loyalty program. With terminal integrated card-linked loyalty, when the customer pays with the enrolled card, the reward is automatically deducted from the total bill and reflected on the terminal printed receipt. It is a seamless and easy experience for the loyalty member and the merchant.

Terminal integrated card-linked loyalty automates the loyalty process, and it is the easiest and best merchant-centric loyalty solution in the marketplace. And there is only one industry that should sell it: ISOs.

Who Better To Sell Than ISOs?

SaaS companies, card brands, and terminal companies are or will be offering terminal integrated card-linked loyalty in 2016, and the ISO is the channel that should sell it. In addition to offering a complementary loyalty revenue stream, ISOs will sell terminal integrated card-linked loyalty to reduce churn. Merchants that have thousands of members in their terminal integrated loyalty program will not want to switch payment processor/loyalty providers.

Because card-linked loyalty touches the payment terminal, the exclusive realm of the ISO, the ISO is the logical sales channels for reselling terminal integrated card-linked loyalty. Welcome back to the Loyalty Game. ***TT***

Jeff Mankoff is the founder and CEO of vPromos Inc., and a member of the ETA Retail Technology Committee. Reach him at jmankoff@vpromos.com.

ADVERTISERS INDEX

Cory Miller

With more than 10 years of IT security experience and several security industry certifications, Cory Miller, director of security operations for ControlScan, oversees vulnerability management, security monitoring, and managed-security services. Here, he discusses setting priorities for data security.

What security priorities should a business set?

Every business has different priorities, but the No. 1 thing is to decide what users can do with your systems before they do. If you apply that philosophy to everything you touch, you'll be pretty successful. The interaction between a user and a system is like a structured conversation. There are specific points you need to cover, and they need to be covered in a certain order. In security, it's much better to lead the discussion than to follow.

Say you were to put up a website where you're selling pictures of your cat. At checkout, you ask users if they want to create an account so you remember them next time. In the form, there's a box for the user's birthday so you can send a coupon around that time. The user types in the year but notices that the cursor is still blinking when he reaches the end. He discovers he can keep typing in numbers or letters, and he does. He holds a key down and puts in thousands of numbers.

That's what I mean by deciding where the conversation goes before the user does. Not everyone is going to use your website the way that you intend. They're going to try the one thing you didn't plan on, and sometimes the results can be disastrous.

What repercussions could that have?

A lot of breaches occur from SQL [structured query language] injection on a website. [That's when fraudsters insert malicious statements into an entry field.] Not having validation and controls in those boxes is a great way to leave yourself open to SQL injection. If it's a box for four numbers, it should only hold four numbers, no letters and no special characters.

What's another top priority?

Reducing your surface area—making your bull's-eye very small. Say you work in an HR office with very personal files on your computer, and down the hall marketing interns are making heavy use of the Internet. Their computers should not influence your computers. If they click the wrong link and download a virus, there's no reason for those two computers to talk. Segmentation in reducing your scope is hugely important.

Planning for failure is absolutely huge. Without some sort of disaster recovery plan and a backup somewhere other than locally, it's very hard to recover. Model the recovery plan on the amount of time you can be down before your business really takes a hit.

What do businesses tend to leave out?

Change management is often overlooked. You need a formal process to review changes you make to systems before you introduce them as well as after.

Patch all your systems on a schedule. Set it up to happen automatically if you don't have the time to do it. If you don't get around to hitting the update button, you'll pay for it.

Is there standard advice that's worth repeating?

This is generic, but layering is very important. There should be a detective control that detects a change if your firewall fails to catch something. There's no one technology that will keep you safe.

What about training?

Security awareness training is the last priority on everyone's list. Train your staff to recognize what an incident looks like and teach them how to respond. It's hard to achieve any security goal without the support of your staff on all levels of the business.

Who should set security priorities?

Business objectives should come from the top, and security priorities should reflect business goals. Senior management should decide the goals and then decide what the acceptable level of risk is. It needs to come top-down but include all levels of the business.

Are businesses doing a good job of setting priorities?

A lot of people are. For health care, there's an increase in Cloud security that helps make medical records electronic. Retailers have heightened mobile security in response to growing use of digital devices. Priorities are shifting as business segments evolve, and that's the way it should be.

What can convince employees to buy into security?

Foster a culture where everyone is responsible for security. If possible, make it fun. If you get up from your computer and you don't lock it, you're going to buy someone lunch. ***TT***

—Ed McKinley

"YOU KNOW THAT CAREER-DEFINING MOMENT PEOPLE TALK ABOUT? GETTING ETA CPP CERTIFIED WAS MINE!"

Natalia Tango
ETA CPP

Earning the ETA CPP credential opened a lot of doors with the right people for Natalia.

Natalia divides her career into Before-ETA CPP and After-ETA CPP. All the effort she put into getting her credential made a remarkable difference. It strengthened her sense of self and validated her as a payments professional. And changed the way others saw her. She gained respect. Opportunities appeared. Her career path improved. Can adding six letters to your name help you move up the ranks? Find out.

Take the next step in your career.
Visit electran.org/etacpp
today to get started.

Only the *CERTIFIED* will *THRIVE!*

ETA CPP™ CERTIFIED PAYMENTS PROFESSIONAL

Celebrating 20 Years of Partnership

Since 1996 we have helped our resellers grow their portfolios. Working together with partners.

That's what we do.

20 YEARS Est. 1996

Authorize.Net®