Exclusive: Read, Learn, and Earn ETA CE Credits PAGE 14

September/October 2017

TRANSACTION *trends*

ETA
THE OFFICIAL PUBLICATION OF THE
ELECTRONIC TRANSACTIONS ASSOCIATION

Defense **Force**

New technology, standards, and tools in the cybersecurity war

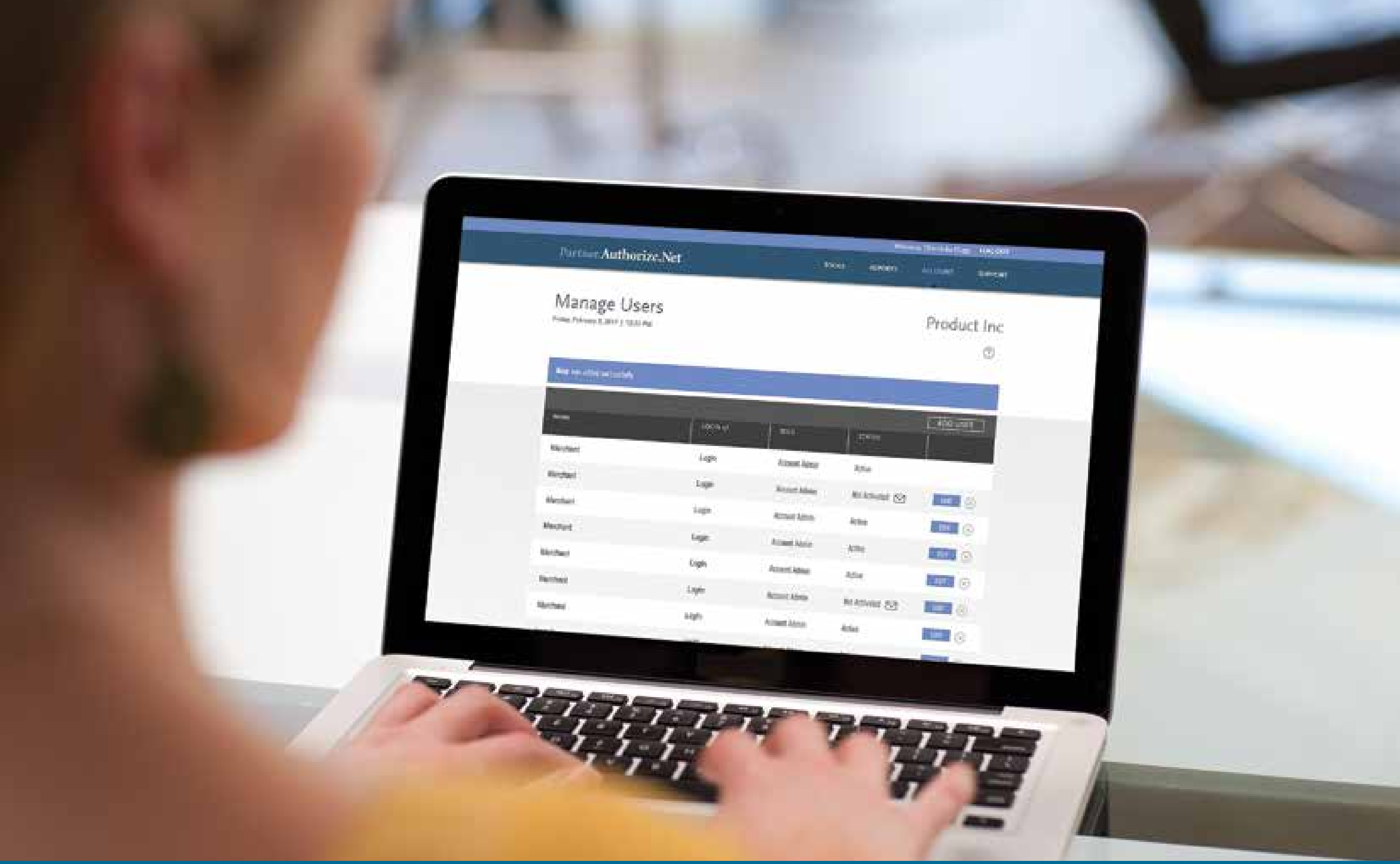
ALSO INSIDE:

Why AI Is Helping—and Hurting—Security Efforts
PAGE 10

Forthcoming PIN on Glass PCI Standard Details
PAGE 14

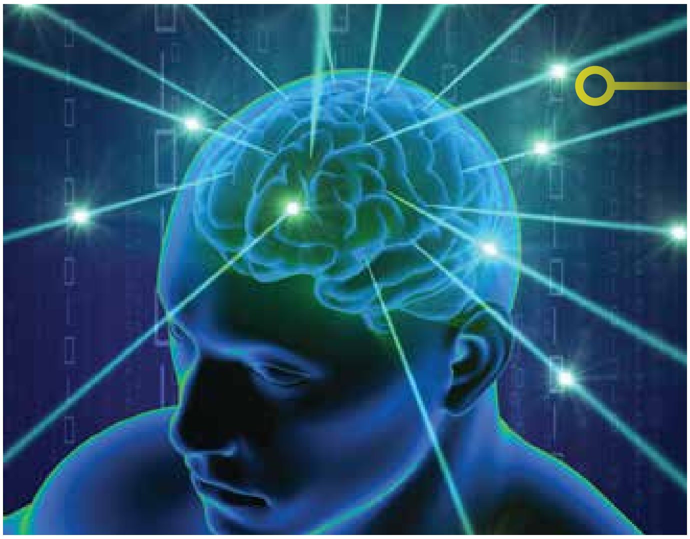
Security Advice for Payment Facilitators
PAGE 18

B2B Opportunities for Acquirers
PAGE 22


Partner.Authorize.Net
Manage Users
Product Inc

contents

The Official Publication of the Electronic Transactions Association Vol. 22 | No. 5



features

departments

Electronic Transactions Association
1620 L Street NW, Suite 1020
Washington, DC 20036
202/828.2635
www.electran.org

ETA CEO Jason Oxman

COO Pamela Furneaux

Vice President, Strategic Partnerships Del Baker Robertson

Director, Communications Meghan Cieslak

SVP, Government Relations Scott Talbott

Vice President, Industry Affairs Amy Zirkle

Director, Regulatory Affairs Philip (PJ) Hoffman

Director, Education & Professional Development Jessica Mosley

Publishing office:
Content Communicators LLC
PO Box 938
Purcellville, VA 20134
703/662.5828

Subscriptions: 202/677.7411

Editor
Josephine Rossi

Editorial/Production Associate
Christine Umbrell

Art Director Janelle Welch

Contributing Writers
Scott Goldthwaite, Ed McKinley, Jared Poulson, Josephine Rossi, Scott Talbott, and Christine Umbrell

Advertising Sales
Alison Bashian
Advertising Sales Manager
Phone: 703/964.1240 ext. 280
Fax: 703/964.1246
abashian@conferencemanagers.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.

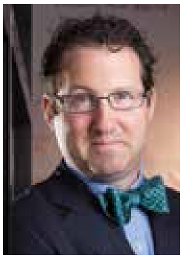
The magazine acts as a moderator without approving, disapproving, or guaranteeing the validity or accuracy of any data, claim, or opinion appearing under a byline or obtained or quoted from an acknowledged source. The opinions expressed do not necessarily reflect the official view of the Electronic Transactions 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 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, 1620 L Street NW, Suite 1020, Washington, DC 20036; 800/695-5509 or 202/828-2635; 202/828-2639 fax. POSTMASTER: **Send address changes to the address noted above.**

@ETA

Welcome to SLF!

Welcome to payments' premier executive gathering, the ETA Strategic Leadership Forum, this year in breathtaking Dana Point, California!



There's no doubt that this is a superior point of contact, where payments leaders step out of the corner office to connect in person. Each year, ETA SLF creates the optimal stage for achieving significant business results—all in a setting fit for the top echelon of a $6 trillion industry. This event is where networking gets to the point, where an executive crowd who knows the value of time can dive into impactful conversations and rise above the small talk.

The payments landscape is changing, and staying informed is more important than ever before. We carefully selected keynote speakers and panelists for this event who are prepared to deliver the high-level information that is meaningful to you. From our keynote round-table illuminating mergers, acquisitions, and the state of payments, to data-driven intelligence from Nielsen on the future of the connected customer, to our closing keynote on how businesses adapt to exponential change, the ETA SLF agenda is designed to foster conversations between frontline leaders, business visionaries, and senior-level industry advocates.

ETA is proud to create events that accelerate payments innovation. All year long, we ensure that our members can stay in touch with collaborators, competitors, partners, and prospects. Less than one month after ETA SLF, on November 9, we're presenting TRANSACT Tech San Francisco. This one-day event brings leading banking, retail, and fintech companies together with innovative startups and venture capitalists. It's the Bay Area's networking event of the year, and I look forward to seeing you there.

ETA never stops working for you, because you never stop working to drive the global economy, delivering seamless, safe, and efficient payments options to merchants and consumers. I look forward to connecting with you at ETA SLF, TRANSACT Tech SF, and future events as we advance electronic transactions together.

Jason Oxman
Chief Executive Officer
Electronic Transactions Association

OF CONTACT

ETA STRATEGIC LEADERSHIP FORUM 2017 | DANA POINT, CA | OCT 3-5 | #ETASLF

ACCESS INDUSTRY LEADERS THROUGH
THE NEW ETA SLF EXPERIENCE.
PERSONALLY TAILORED, CONCIERGE-DRIVEN.

ETA's Strategic Leadership Forum is the curated payments event that connects the leaders of today and tomorrow—from C-suite veterans to emerging innovators. Reimagined in 2017, SLF facilitates introductions and personalizes itineraries to accelerate your business objectives in an exclusive oceanfront setting. Cut through the industry noise by getting to the point. Register today at electran.org/slf17.

ETA STRATEGIC LEADERSHIP FORUM

POWERFUL FIGURES. EXPONENTIAL RESULTS.

STRATEGIC LEADER PROFILE

WOMPLY'S TURNING POINT

"Womply attends SLF year after year because it puts us at the same table with key players in payments. Last year, we were able to take a deal over the one-yard line over lunch with a major card company. You look around SLF and meetings like this are happening everywhere."

–Cory Capoccia, President, Womply

PCI Compliance ‘Critical Link,’ Says Verizon

Businesses that pursue compliance with guidelines from the PCI Data Security Standard (DSS) are much more likely to avoid cyber threats than noncompliant companies, according to Verizon’s “2017 Payment Security Report,” released in late August. Verizon studied approximately 300 breaches that occurred between 2010 and 2016, and found that none of the breached organizations were fully compliant with PCI DSS at the time a breach occurred. Some of the breached companies had noncompliant firewalls, passwords, and antivirus software and network monitoring and policies, according to the report.

“There is a clear link between PCI DSS compliance and an organization’s ability to defend itself against cyberattacks,” said Rodolphe Simonetti, Verizon’s global managing director for security consulting. Overall, PCI compliance is increasing, with 55 percent of the surveyed companies meeting the benchmark, up from 48 percent in 2015 and 11 percent in 2012. However, “the fact remains that over 40 percent of the global organizations we assessed—large and small—are still not meeting PCI DSS compliance standards,” said Simonetti. Verizon also found that nearly half of the companies that pass validation fall out of compliance within nine months.

Consumers prefer interacting with compliant companies, according to the report; 65 percent of respondents reported they would be unlikely to do business with an organization that experienced a breach where their financial and sensitive information was stolen.

Analyzing results by company sector, IT companies were the most likely to achieve full compliance, with 61 percent achieving full compliance during interim validation. Fifty-nine percent of financial services organizations, 50 percent of retail companies, and 43 percent of hospitality companies achieved full compliance.

P2P Gains Momentum Among U.S. Consumers

Forty-seven percent of consumers surveyed via a recent U.S. Bank Cash Behavior Survey prefer the use of digital apps, rather than cash, to make payments. More Americans are leveraging apps such as Zelle, Venmo, and Square Cash to remit funds digitally.

Younger consumers are even more likely to use digital apps to make payments: 49 percent of millennials and 44 percent of Generation X have done so, while only 32 percent of baby boomers have engaged in digital payment activities, according to the survey results.

The rise of person-to-person (P2P) apps to facilitate the transfer of money via mobile devices has led to fewer Americans carrying cash. Fifty percent of survey respondents report carrying cash less than half of the time. “The incredible consumer response to digital and mobile banking solutions is changing the entire industry and diminishing the historic use of cash,” said Gareth Gaston, executive vice president of omnichannel at U.S. Bank. “ATM withdrawals and branch visits are slowly declining, while mobile transactions are increasing dramatically year over year.”

Seventy-three percent of respondents are more likely to use a P2P service if payments are secure and backed by a bank, and 78 percent are more likely to use P2P if they can access funds almost immediately, according to the survey results.

Contactless Transactions To Grow—Even in the U.S.—By 2022

Fifty-three percent of global transactions at the point of sale (POS) are predicted to be contactless within five years—a drastic rise from 15 percent in 2017, according to a new report from Juniper Research.

Contactless infrastructure and deployments have scaled rapidly in developed markets over the past two to three years, according to the whitepaper "POS and mPOS Terminals: Our Vision for 2022." With both Visa and Mastercard mandating that terminals in some markets be contactless-enabled by 2020, the trend is expected to continue. Juniper predicts that by 2022, markets in Brazil, Canada, Japan, South Korea, and Western Europe may have 100 percent penetration of contactless-enabled POS terminals.

Adoption of contactless payments in the United States is moving at a slower pace but is gaining momentum, given the recent migration to EMV. "While U.S. card issuers haven't yet made contactless a priority, the extremely positive response across Europe, both from merchants and consumers, suggests the U.S. would see very rapid migration at POS if and when contactless cards become mainstream," reported Windsor Holden, PhD, Juniper research author.

The expectation that U.S. financial institutions will offer more contactless cards also factors into the expected rise in use. "Assuming that the banks increasingly offer contactless cards over the 2018-2020 period, we believe that cards will have overhauled smartphones by 2022 to become the predominant mechanism for contactless payment in the U.S. by this time," according to the whitepaper.

Globally, Juniper predicts that nearly 170 billion contactless transactions will occur in 2020, generated by a combination of card, mobile, and wearable transactions—an average annual increase of 38 percent.

Infographic

Younger Consumers Dominate Market for In-App Purchases

Percentage of U.S. consumers who have made in-app purchases over the past year

	No In-App Purchases	1-4 In-App Purchases	5 or More In-App Purchases
Age 18-34	36%	28%	36%
Age 35-54	66%	26%	8%
Age 55+	80%	17%	3%

Source: "The 2017 U.S. Mobile App Report," comScore, 2017.

Fast Fact

Thirty percent of millennials say the credit card is their **most frequent payment method**, compared with 43 percent among their older counterparts.

Source: "Small Business Banking for Millennials: How Banks Can Attract and Serve the Largest Generation in History," Javelin, June 2017.

E-Commerce on the Rise Despite Persisting Security Concerns

While many consumers are turning to online and mobile technology to make purchases, they also are likely to halt transactions over security fears, according to the recently published "2017 American Express Digital Payments Survey."

Eighty-one percent of U.S. merchants that have both e-commerce and brick-and-mortar stores view the online and mobile sales channel as the biggest growth opportunity for their business, according to the survey, which polled both consumers and merchants about online shopping habits. Seventy percent of merchants say the proportion of their annual sales generated via online and mobile transactions has increased over the previous year.

Nine in 10 consumers report having made at least one online purchase in the past 12 months, and 73 percent have made three or more online purchases, according to the survey findings. Almost half (47 percent) have increased the frequency of their online purchases in the past year. More than 70 percent say they have used a digital payment option, such as a mobile wallet, P2P payment app, or one-click checkout button, to complete a purchase.

While digital sales are robust, 37 percent of consumers who have made three or more purchases in the past year have abandoned an online purchase because they did not feel their payment would be secure, according to the report. This finding suggests merchants that take steps to reduce fraud and enhance security may have an opportunity to capture a larger share of consumers' online spending. "Digital innovation is enabling consumers to buy from merchants when and where it's most convenient for them," said Mike Matan, American Express's vice president, industry engagement, product and marketing, Global Network Business Division. "But the results of our survey show that for merchants to capitalize on consumers' continued shift to online and mobile commerce, they need to provide their customers with the confidence that their information is secure."

Moves & Mergers

Blackhawk Network has acquired CashStar Inc., a provider of digital gift card commerce solutions. With the acquisition, CashStar has become part of Blackhawk's digital and incentives businesses.

ETA welcomed **Elizabeth (Liz) Ryan**, executive vice president and wholesale merchant services segment executive at Wells Fargo, to its board of directors. A 30-year veteran of the financial industry, Ryan was appointed in 2016 to lead and transform the newly created wholesale merchant services segment at Wells Fargo, which includes more than 200 team members serving a diverse group of customers that generate more than $320 billion in card volume processed annually.

PayPal Holdings has agreed to acquire online lending company Swift Financial. The acquisition will allow PayPal to offer loans to larger businesses that process payments through its platform and better provide credit to firms that are not yet users of its services.

Global payment processing company **Pivotal Payments** announced that **Allan Lacoste** has joined the company as vice president. Lacoste has more than 20 years of leadership experience and will be responsible for managing the overall growth of Pivotal's North American sales divisions. He most recently served as ISO director at Total Merchant Services, where he headed up its ISO and sales partner channel.

Visa Inc. has appointed **Charlotte Hogg** as executive vice president and CEO for its European operations, effective October 1. She will join the Visa Europe Limited board of directors and will also be a member of Visa's global executive committee. Hogg brings more than 25 years of experience to Visa, most recently serving as chief operating officer for the Bank of England.

Fall Outlook

States and regulators home in on payments

Scott Talbott

On any given year in Washington, Congress is in session for a relatively short period of time—about 150 days on average. Consequently, for any legislation to advance, the administration and Congress need to move it very quickly. As 2017 winds down, we have not seen many bills move over the goal line, and, other than tax reform, the prospects for payments industry legislation are dimming. However, that doesn't mean the policy arena is quiet. Two areas—federal regulators and states capitals—have seen much activity.

Regulatory Changes

The president has or will soon appoint new leadership at the federal regulators to supervise financial institutions and their fintech partners. These bodies also write and enforce the regulations that govern the products, management, and strategy of financial institutions and their fintech partners. These include the Office of the Comptroller of the Currency (OCC), which oversees national banks; the Federal Deposit Insurance Corporation (FDIC), which oversees deposits at banks; the Consumer Financial Protection Bureau (CFPB), which oversees consumer protections; the Federal Reserve, which oversees banks and monetary policy; and more. These regulators can encourage economic development or deter it altogether. Finding the right amount of regulation is essential to a strong economy. Here are two current examples of how regulations shape the payments industry:

- **The OCC Fintech Charter.** The OCC has proposed a new charter for fintech companies. A federal charter would allow a startup to avoid the costly and time-consuming process of getting a license in each of the 50 states. One charter would also allow a start-up to have a nationwide presence, allowing the benefits of its new product or service to be available to all Americans.
- **Death of Operation Choke Point (OCP).** One way to encourage economic development is to remove a barrier. Attorney General Jeff Sessions has confirmed that OCP is no longer a policy initiative for the Department of Justice. The OCP program pressured payments companies to "choke-off" the ability of politically disfavored merchants to access the payments system. With the death of OCP, payments companies can resume working with all merchants.

Increased State-Level Activity

We've seen a dramatic increase in interest by individual states aimed at the payments industry. Three major themes shape their approaches: imposing new taxes or expanding the tax base; applying existing laws to new fintech-inspired developments; and altering the way the payments industry does business. The activity of the states has the real possibility of affecting the bottom line and seamless operation of the payments system.

Many states are strapped for cash, as state budgets are stretched thin. As a result, a number of states are looking to impose new taxes or expand the base, which means applying existing taxes in a new way. The tax is focused on money transition—sending payments home or new peer-to-peer money.

The state of Washington is expanding its base by applying an existing tax in a novel way to payment processors. Earlier this year, the state's Department of Revenue issued an Excise Tax Advisory declaring that the merchants, discount was taxable income to processors. This is a new application of the state's Business & Occupations Tax.

Many states proposed imposing new taxes or increasing existing tax rates throughout 2017. These states include Georgia, Louisiana, Iowa, and Oklahoma. Each of these states considered proposals to increase the state's existing tax on money transfers.

Modernizing Regulations To Address Fintech

Many states are eyeing the deployment of new products and services and are examining ways to regulate them. Unfortunately, many times the only tools in their toolbox are existing laws that were written before the new products and services existed. A number of state policy makers spent time during 2017 trying to apply existing laws to developments in the payments space or working to try and modernize their laws.

Georgia introduced a bill designed to make it easier for drivers in ridesharing services to pay taxes. However, an early draft of the bill would have made payment processors liable for services provided by ridesharing drivers because they process the payments. The language was ultimately removed in a later version of the bill, but the fact remains that as states attempt to modernize regulations to address fintech and other innovations, there is a risk of unintended consequences that can affect any number of industries.

One positive area is that six banking regulators in New England states are working to create a compact to allow a fintech company chartered in any of the six states to receive a lighter regulatory approach that reflects its startup status. The creation of a sandbox or greenhouse is designed to reduce the hurdle complying with existing regulations poses to startups. This collective and collaborative approach creates a positive environment to encouraging growth and innovation.

Altering the Role of the Payments Industry

The final way that states are affecting the payments industry is by attempting to change the role that the payments industry plays. In Massachusetts, the governor signed a law that asks payments processors to calculate, collect, and remit a merchant's sales tax liability on a daily basis. Currently, merchants in Massachusetts perform these steps on a monthly basis. This change asks the payments industry to step in between merchants and the state, which raises many concerns.

A comprehensive look at the forces that shape policy extends beyond Capitol Hill and includes federal regulators as well as state policy makers. Each of these entities forms a patch quilt of tiles that form the mosaic of public policy for the remainder of this year and next. ***TT***

Scott Talbott is senior vice president of government affairs at ETA. For more information, please contact Talbott at stalbott@electran.org or Grant Carlson, government affairs specialist, at gcarlson@electran.org.

Fighting the Good Fight

How AI is fueling both sides of the cybersecurity arms race

By Ed McKinley

Ominous-looking aircraft patrol a dark and eerie sky, hovering now and then to fire a laser blast down at a ragged soldier scampering through the ruins of Los Angeles. Nearby, a gigantic armored vehicle rolls across the scorched earth, crushing the human skulls that litter the scene. It's the dystopian future of the year 2029 depicted in the opening scene of *The Terminator*, the 1984 film that has enthralled generations of movie fans. The premise is that advanced machines are waging war to exterminate humanity.

Yet, who can forget the lighthearted banter of C-3PO and R2-D2, the affable android-robot duo in the original 1977 *Star Wars* movie? The pair provided comic relief to prevent the audience from overdosing on the strife among the humans "a long time ago in a galaxy far, far away," as the setting is described in the movie's opening crawl.

Outside of the Cineplex, man's interface with artificial intelligence (AI) falls somewhere between those extremes of menace and frivolity. In the payments industry, AI is pitting good guys against bad guys. Thieves employ the technology in their quest to steal card data and transaction history, while the payments industry develops similar methods to foil their schemes. Some describe it as an arms race between good and evil.

But it's a battle where the right side isn't always winning, according to Adam Frisch, CEO of Buy It Mobility Networks, a company with offices in New York City and Atlanta that uses the automated clearing house (ACH) network to create "private label debit" on a customer-engagement platform. "Mobile transaction fraud is around 7 percent to 8 percent on average," he says. "We know of two very well-known national brands that are actually losing money on mobile because of fraud."

Online fraud attacks increased 8.9 percent over the course of 2016 as the spread of EMV pushed criminal activity out of brick-and-mortar stores and onto the internet, says Forter CEO and Cofounder Michael Reitblat, citing the company's most recent global fraud report compiled by the Merchant Risk Council. Forter is a fraud prevention technology company that helps retailers approve or decline digital transactions.

Criminals are using AI to predict what websites consumers will visit or where they'll use their phones to purchase

goods and services, says one vendor, who requested anonymity to avoid identification with criminal elements. By becoming the "man in the middle," crooks are able to steal personal and payment credentials and use them for fraudulent transactions, the vendor adds.

Fraudsters employ AI to probe defenses at financial institutions by using stolen credentials to make illicit transactions as small as a dollar and then increase the amount, says Steve Durney, senior vice president of issuer relations at Ethoca, a Toronto-based software as a service provider that helps 6,000 merchants and 500 card issuers work together on its network to combat fraud. Criminals are probing networks to discover if the card is still active and what amount is the limit for not raising suspicion, he notes.

Lawbreakers also use seemingly legitimate electronic transactions for money laundering, the phrase that describes erasing the taint of ill-gotten gains from activities like smuggling illegal drugs, notes Anand Rao, an AI expert and a partner at PwC Advisory, the international audit, tax, and consulting company. The government expects financial institutions to detect and report money laundering, he notes.

The Enemy

"The criminals—since 2000—have certainly raised their level of sophistication," says Durney. The large breaches, including those at Target and Home Depot, have been well-document-

"THE MOST UNBELIEVABLE THING ABOUT THESE INSTIGATORS IS THAT **THE VAST MAJORITY OF THEM DON'T CONSIDER THEMSELVES CRIMINALS.** THEY CONSIDER THEMSELVES OPPORTUNISTS AND SAVVY BUSINESS PEOPLE."

—Michael Reitblat, Forter

ed, he notes. "The criminals have introduced what I would say is almost formal procedure and process of how you monetize and operationalize the thefts," he says.

Crooks visit the "dark net" to buy stolen credit card information for perhaps $1.50 per identity, or they spend $5 or sometimes much more for data on purchasing habits they can use to target consumers for scams that range from fake travel vouchers to real-world home burglaries when transaction history indicates the owners are out of town, according to Monica Eaton-Cardone, COO and cofounder of Chargebacks911, which provides a risk management and mitigation platform and software as a service. Knowing a consumer's purchasing behavior enables criminals to make transactions that seem "reasonable" and thus go undetected, she says.

The "dark economy" is booming in cyberspace, and fraudersters are leveraging tech and AI to steal and use data, Reitblat says. Denizens of that cyber underworld automate the process of using stolen identities to make fraudulent purchases from numerous merchants at once, he maintains. "The most unbelievable thing about these instigators is that the vast majority of them don't consider themselves criminals," he notes. "They consider themselves opportunists and savvy business people."

In that virtual underground, some cyber criminals specialize in services to other cyber criminals, observes a vendor who asked not to be named. Some organizations focus on breaches; others concentrate on consolidating data on identity; and still others develop expertise in perpetrating transaction fraud. "It's almost like you outsource what you need," the vendor says. "They sell information back and forth."

Eastern Europe and parts of Africa have earned reputations as centers of criminal hacking, identity theft, and social engineering, while Brazil seems to harbor more than its share of gas-pump skimmers, says Durney. As the scene becomes more dispersed, we're seeing online criminals in Asia and the United States as well, he adds.

The Ally

To retaliate against that demimonde of online hoods, the payments industry is exercising at least one aspect of AI—machine learning. Machine learning occurs when computers observe and learn from patterns they perceive, says Rao. AI represents a giant step beyond directing computers to follow rules-based criteria laid out by humans, he contends.

"As soon as you delve into the e-commerce world, to stay competitive and keep up with fraud, you have to utilize machine learning components and AI technology in order to adapt," says Eaton-Cardone.

Machine learning, sometimes called ML, occurs when computers analyze data given to learn on their own and then do something they weren't programmed to do, says Reitblat. It happens when a machine can use data from the past to look at fresh data and predict a result for that new data. For example, knowing about past transactions should enable a machine to make predictions about whether a new transaction will prove to be fraudulent or genuine, he says.

Depending upon one's definition of ML, the payments industry has been using the technology for a number of years, perhaps as early as the early 2010s, says Durney. "Moore's law takes over where you have a doubling of capacity to churn through information every year," he says, referring to the observation Intel Cofounder Gordon Moore made in 1965 that the number of transistors per square inch on integrated circuits had doubled every year since their invention.

ML constitutes one aspect of what's considered AI, the emerging ability of computers to "think" like their human creators. The general definition of AI tends to change over time. Many regard it as a description of whatever developments have come most recently in cyber evolution, says Reitblat. He quotes a Gartner report to shed light on the real meaning of the often-used terminology: "The artificial intelligence acronym 'AI' might more appropriately stand for 'amazing innovations' that do what we thought technology couldn't do." The quotation comes from a Gartner piece entitled "A Framework for Applying AI in the Enterprise," according to Reitblat.

However one defines AI or ML, pasting the technology onto an aging system won't meet today's needs, says Frisch of Buy It Mobility Networks. His company embeds AI and ML throughout its platform, using the technology when the customer comes onto the platform and while transactions occur, he maintains.

In payments, AI and ML comprise "three basic components," Frisch explains. "We have to gather the right data, analyze the data correctly, and then apply the data to achieve the optimal outcome for the consumer and merchant." Using those components effectively requires a balance between controls that are too tight, and thus disallow valid transactions, and too loose, which consequently permit fraud to occur, he notes.

To accomplish that, Buy It Mobility Networks uses the enrollment process to amass thousands of data points on each shopper, the shopper's payment credential, and the device the shopper uses to pay. That information feeds into a risk-scoring engine that dictates how the system will monitor a consumer's transactions. "Our system is constantly getting better at identifying trends," he says. "If this data point corresponds to that data point, then it's fraud. We recognize patterns." After enrollment, computers track where and how consumers make transactions to spot anomalies that may indicate fraud.

In general, financial institutions are improving their response to fraud by eliminating the silos of data that in the past may have separated bits of information, says Durney. "A couple of banks are doing an exceptional job of looking across multiple verticals," he maintains, creating usable information quickly. That way, they can "pattern" activity to spot dubious trends, he adds. "It's cat and mouse or whack-a-mole," he opines. "You stop one, and the next one pops up."

"IT'S **CAT AND MOUSE OR WHACK-A-MOLE**. YOU STOP ONE, AND THE NEXT ONE POPS UP."

—Steve Durney, Ethoca

Machines not only have to detect fraud, they have to do it in ways that humans can explain to each other, notes Rao. That way, financial institutions can describe to regulators exactly how criminals are illegally gaming the payments system, he says.

But the machines can't do it all when it comes to fighting fraud, sources agree. "At Forter, we combine machine learning and human creativity to accurately prevent fraud at any scale for prominent e-commerce clients … our machines—guided and refined by our team of human researchers—effectively detect and prevent the vast majority of fraud accurately by learning to anticipate what fraudsters will do next," says Reitblat.

The Humans

That coalition of man and machine seems likely to stay busy dealing with fraudsters for the foreseeable future, sources agree. As payments technology advances at a rapid pace, innovations are thoroughly tested in theory but—by definition—can't be tested in the real world until they're introduced into the real world, notes Eaton-Cardone of Chargebacks911. That provides opportunities for criminals who are working hard to keep up with change, she notes, describing the situation as a "petri dish for fraud." Apple Pay, for example, succeeded only after the criminal element greeted the payment method's introduction with an avalanche of fraud, she says.

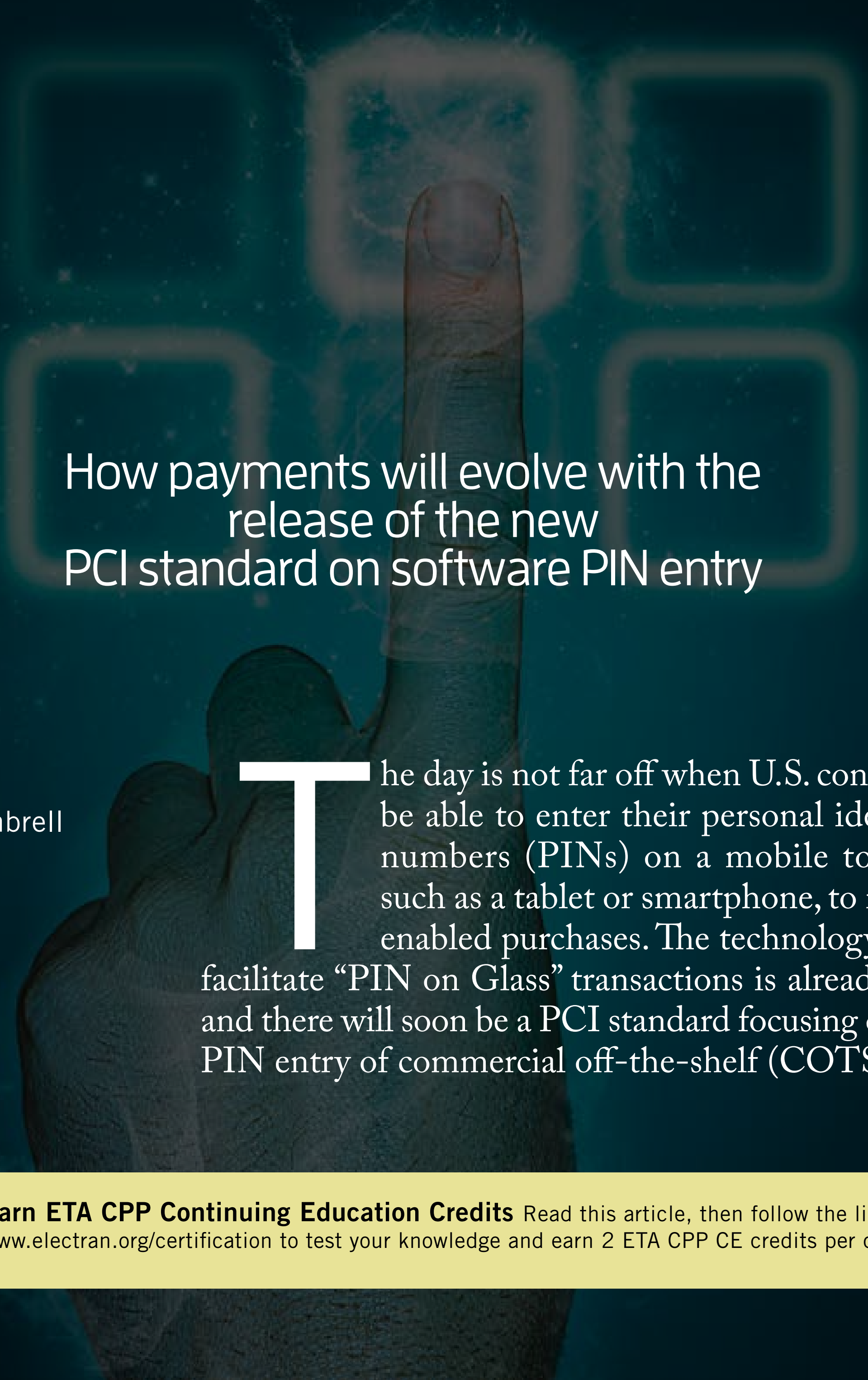
The welter of complexity in the payments world also keeps the industry's security community up at night, says Eaton-Cardone. More than 200 types of electronic payments—including everything from loyalty points and bank transfers to virtual cards and cash-back schemes—have come into use worldwide, and a third of them are less than six months old, she notes.

Meanwhile, the dark side of the transaction scene has proven resilient. When the industry closes a door to criminality, criminals tend not to make a career change and seek a job as a barista at Starbucks, says Durney. Instead, they adapt to the change and keep working to penetrate the defenses of the payments industry. The AI arms race continues. ***TT***

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

Next-Gen **PIN** on Glass

How payments will evolve with the release of the new PCI standard on software PIN entry



By Christine Umbrell

The day is not far off when U.S. consumers will be able to enter their personal identification numbers (PINs) on a mobile touchscreen, such as a tablet or smartphone, to make PIN-enabled purchases. The technology needed to facilitate "PIN on Glass" transactions is already available, and there will soon be a PCI standard focusing on software PIN entry of commercial off-the-shelf (COTS) devices.

ETA CPP CERTIFIED PAYMENTS PROFESSIONAL

Earn ETA CPP Continuing Education Credits Read this article, then follow the links on http://www.electran.org/certification to test your knowledge and earn 2 ETA CPP CE credits per quiz!

"PIN on Glass technology has been around for a long time," says Troy Leach, chief technology officer for the PCI Security Standards Council. "The concept is not new." What is new is the concept of software PIN entry into a COTS device not dedicated exclusively for payment, says Leach.

The Council is preparing to open a request-for-comment period for a new standard in October 2017, when participating organization members will be invited to review and offer feedback on a standard for software PIN entry. Depending on the comments generated, the standard could go public as early as December of this year, according to Leach.

PIN 2.0

While it may seem that transitioning to PIN on touchscreens would be a logical next step at this time, it's "a surprisingly complex topic," says James Wester, research director of global payments, International Data Corp. Accepting PIN on a mobile device "seems so simple—but if you look at all of the things that go into it, it becomes complex."

Without software PIN entry, mobile transactions require a secondary PIN-entry device—and it is "both expensive and clunky to have two devices" to facilitate transactions, maintains Wester. "Being able to combine everything in a single package is a more elegant, better design, and it removes friction in the payment process."

The movement to software PIN entry on COTS devices is "an incremental step in the mobile device becoming more and more a part of payments being mobile," Wester adds. "The way we pay and the way payments are accepted have changed so much in the past five years." Several different types of companies are now involved in the payments value scheme, from issuers to networks to acquirers, and both hardware and software vendors, says Wester. Changes in EMV, mobile payments, and new ways to shop and pay have all played a part in the progression of payments—as will software PIN entry, he predicts.

The shift being addressed by the new standard is a movement away from traditional PIN on Glass solutions—which typically require hardware attachments—toward new solutions that may allow for off-the-shelf tablets or smartphones to accept PIN numbers in a secure and "isolated" manner, according to Leach. "Before the PIN is entered via 'Glass'—or software—the Primary Account Number (PAN) is already encrypted and cannot be decrypted," he explains. When the new standard is released, it is expected to focus on software requirements for payment applications that manage transactions within COTS devices.

The New Standard

The Council's software-based PIN entry standard—one of seven new and existing PCI standards being released or updated this year—looks at how to separate the PIN from any other type of account information. Isolating the PIN from any other data may prevent future fraud attacks that would correlate payment data from multiple locations, according to Leach. "We've relied on the integrity of PIN authentication for decades," he says, and the new standard will allow innovators to isolate the PIN data for new uses without compromising that integrity.

There are three central components to the proposed standard, according to Leach:

- **Isolating PAN from PIN**. "We are looking at software requirements for payment applications that manage transactions within the COTS device," says Leach. "To create isolation, you need to be able to enter an account number in such a way that it can't be decrypted in a COTS device."
- **Software security.** This is key to protecting the integrity of handling applications with PINs in a COTS device. "A COTS environment is inherently insecure," Leach acknowledges, so security must be augmented to ensure PIN data remains protected.
- **Monitoring.** Remote monitoring should be carried out by an independent party to confirm that the software, COTS device, and transaction have integrity and behave as expected, and to look for any types of suspicious activity. "There needs to be ongoing security and monitoring to ensure that the device itself is not compromised," says Leach.

"It's really about isolating," Leach says. As dynamic data and dynamic authentication take hold, they diminish the value of account information for future payment considerations. "If you're using EMV Payment Tokens or multifactor authentication, the importance of PIN security will diminish because it won't be the only verification for the transaction, which is why PIN security has been so rigorous to date," Leach explains. "It is the primary verification in an environment that co-hosts with account number and other sensitive data."

Secure Solutions

As new software PIN entry solutions are developed, protecting cardholders' PIN numbers is of utmost importance, says Scott Spiker, founder of Cipherithm, principal partner at Rockledge Group, and chair of Working Group X9F6 of the Accredited Standards Committee X9 Inc. (X9), which develops and maintains standards for the financial services industry. PINs offer a gateway to money, rather than simply products, notes Spiker. Cyberthieves who are able to identify a PIN associated with a card could theoretically access cash from an ATM. "There's real money involved—not just merchandise," says Spiker.

Currently, the security surrounding the PIN is "quite robust" and in compliance with X9 regulations, says Spiker.

🔊 Learn more about the current state of PIN on Glass and the opportunities it presents. Log in and listen to "PIN on Glass Security: To Touch or Not To Touch, That Is the Question" from TRANSACT at www.eventscribe.com/2017/Transact.

ANSI/ISO standards require that PIN handling devices used by processors and acquirers be secure cryptographic devices (SCDs). But those standards apply to hardware, whereas the new PCI standard addresses software.

According to Leach, the ANSI/ISO standards are written for an environment where PIN entry is handled in the same environment as the account data is entered, while the new standard addresses mobile transactions where "the account information will never be used in the same environment as the PIN." This means that the standard likely will be designed for chip transactions only, and will not allow for magstripe transactions, to ensure the account information remains isolated from the PIN number, Leach says.

Some of the security challenges may be balanced out by the advantages of software PIN entry, according to proponents of the technology. Software is inherently nimble and may be updated quickly, allowing for remote updates that can address the newest cyber attacks as they are introduced. "Merchants want a simple solution," states Leach. "We need to simplify and eliminate the risk for merchants. One way we do that at the PCI Council is by point-to-point encryption," he says. Software PIN entry offers a new way to isolate the merchant from the risk of that transaction.

In addition, COTS devices that are enabled with software PIN entry may provide more opportunities in the coming years, contends Leach. Integrating software security and third-party monitoring requirements in the standard offers "an opportunity to provide more payment channels for more merchants" and provides a platform for new ways to authenticate, he says.

What's Next?

Once the standard is released, it is unclear how soon new solutions will become compliant and introduced to the market.

Current software PIN entry models are being tested and implemented in other countries, via Visa's mobile chip-and-PIN pilot program in Australia and Britain, and AEVI's Albert device in Australia (see sidebar). But "none of the current pilots being conducted have any association with the PCI Council," says Leach. "I would imagine there are several solutions in the marketplace today" that may one day be compliant with the upcoming PCI standard on software PIN entry, but "it's too early to tell if any solutions available today can meet the standard," he explains. "As we design requirements for long-term deployment, we should not assume that an existing process today will meet all security controls of the standard."

The significance of the standard is that it will "introduce new opportunities to think about security and authentication," says Leach. Building on recent security advances engendered by EMV chip and encryption, isolating the PIN for use on mobile COTS devices offers another way to protect consumers while leveraging new technologies, Leach explains. "Can we create new types of integrity so we can remain confident that cardholders are who they say they are?" he asks. "We've had a problem with confidentiality—keep-

PIN on Glass Overseas

It is unclear whether any currently available products will meet the requirements of the soon-to-be-released PCI standard focusing on software personal identification number (PIN) entry of commercial off-the-shelf (COTS) devices. But two companies—Visa and AEVI—are garnering buzz in the "PIN on Glass" sector.

Visa is reportedly in the midst of a mobile chip-and-PIN pilot program in Australia and Britain. The program, which tests a Square reader that works with a chip and PIN—with the PIN entered onto a smartphone screen—is tentatively scheduled to run through 2018. "At this stage, the technology is performing well within our expectations," Sam Gianniotis, head of risk for Visa in Australia, New Zealand, and the South Pacific, recently told the *Financial Review*. "We fundamentally believe that mobile point-of-sale is a payment innovation that adds value to financial institutions, merchants, and consumers."

AEVI, on the other hand, introduced "Albert"—an Android-based tablet with an integrated, encrypted PIN pad, card reader, and receipt printer—in Australia in 2015. There are now more than 100,000 devices on the market across Europe and Australia, says Martina Jeronski, head of marketing and communications at AEVI. Albert was "the first certified, single-screen device taking payments with PIN on Glass, with an open app marketplace," says Jeronski. Albert is connected to an open, but secure and controlled, marketplace that contains dozens of B2B apps supporting a variety of merchant use cases, she explains. "App content is key. This approach allows the AEVI-enabled devices to be leveraged in a variety of different, more tailored, merchant scenarios—hairdressers, car dealers, doctors, and coffee shops are just a few examples where Alberts are in use today."

The company focuses on maintaining high levels of security by ensuring its devices are connected to AEVI's marketplace and receive security updates on a regular basis, says Jeronski. "We make sure acquirers have complete control of their own environment. Security is not restricted to payments alone, as it also applies to the app content." AEVI aims to enable banks, acquirers, ISOs, and VARs to create unique merchant offerings with a choice of hardware and app content for their preferred merchant verticals. "PIN on Glass enables commercial off-the-shelf devices—not just dedicated payment devices—to take secure payments," Jeronski says. "This means we can fulfill even more tailored use cases at the point of sale."

ing information from getting into the hands of criminals." Isolating the PIN can devalue cardholder information and reduce the chance of that data being used for fraud in other payment channels by cyberthieves.

Wester believes that once the standard is released, the technology will have a greater impact on merchant implementation than on consumer behavior. "The idea of entering a PIN to make a purchase is not really something [the consumer] thinks as much about," he explains. In fact, many consumers already seem comfortable using signature rather than PIN verification when requested by merchants. But if consumers aren't focusing on security, merchants will need to do so, says Wester.

Spiker notes that "any software-based systems have the possibility of being attacked." And Wester wonders whether it will be possible for cybercriminals to try to write apps to steal PIN data. But security will continue to be of utmost importance as the new standard is introduced and new products come to market.

"Those companies providing the services" are thinking about all of the security issues, says Wester. Having a PCI standard in place will help ensure companies offer secure solutions. "Certain things are hard to predict, and some bad guys may try to find ways to exploit new technologies. But everyone is paying attention to security."

An Eye on the Future

The arrival of solutions that allow software PIN entry on COTS devices is imminent, but where this road will lead is yet to be seen. With so much going on in the payments space, "it's going to be hard to predict whether we'll start seeing applications" once the standard is released, says Wester.

"Things evolve over time," says Leach. "This standard is future-looking." This is a change over how payments have evolved in the past, he says. "Very often, we try to retrofit old security practices with new technology. But we need to be as innovative with security so that our protections can address modern threats and do not become a laggard for the next generation of payments."

The release of the standard will facilitate the exploration of "new ways we can innovate the technology," says Leach, "to make payment data more secure for merchants." ***TT***

Christine Umbrell is a contributing writer to Transaction Trends. *Reach her at cumbrell@contentcommunicators.com.*

SECURITY AND THE PAYMENT FACILITATOR

Why unprecedented growth means vigilance is more important than ever

By Ed McKinley

In the payment facilitator model of merchant acquiring, security must be a priority from the very beginning of the process. In other words, onboarding procedures are the first place to guard against granting payment services to a criminal bent on committing transaction fraud, industry sources agree.

"As you remove friction from the signup process, you need to make sure that you put in place other security so that bad actors aren't creating fake merchant accounts," warns Dave Duncan, president of ProPay, a TSYS subsidiary that provides services to payment facilitators. "You don't want to set up a solution for fraudsters to be able to process stolen cards."

Payment facilitators—acquirers that aggregate submerchants under one or just a few merchant identification numbers (MIDs)—are increasing in number prodigiously these days, says Todd Ablowitz, president of Colorado-based Double Diamond Group and publisher of PaymentFacilitator.com. To some extent, payment facilitators are supplanting the ISO model of assigning an MID to each merchant and offering unadorned payment services, industry sources agree.

But payment facilitators have proliferated not only because they're disrupting the ISO ways of going to market but also because they're enabling tiny businesses—everything from farmers' roadside tomato stands to afterschool lawn-mowing services—to accept credit cards as payment for the first time, says Derek Schultz, director, payment partner programs for Trustwave, a managed payments security technology company.

Where do the new payment facilitators come from? Independent software vendors (ISVs) become payment facilitators when they add payments to the business functions of the products they provide to merchants, according to Dustin Young, a spokesman for Infinicept, which provides automated services to payment facilitators. Meanwhile, ISOs become payment facilitators when they begin aggregating merchants, often as they add such business functions as scheduling or inventory control to their transaction services, he notes.

Perhaps as many as 10,000 ISVs have become payment facilitators in the last two years, Schultz says. He adds that some have been in the software business for years and simply incorporate a payment switch into the background of their offering and link with a gateway. "It's that easy," he says.

Ablowitz agrees that the influx of ISVs has reached staggering proportions. "Many, many, many" ISVs have become payment facilitators, he says. Meanwhile, lots of ISOs are transforming themselves into budding tech companies to join the ranks of payment facilitators, he observes.

Keeping Pace

But fierce growth brings complications. Payment facilitators must remain vigilant to avoid mistaking criminals for legitimate merchants because the industry is expanding rapidly as more micro merchants begin accepting payment cards, sources say. In some ways, today's payment facilitator scene reminds Duncan of 25 years ago when cards were first becoming widespread—the market was expanding rapidly in both cases.

Still, the two periods of card-acceptance proliferation differ in important ways, Duncan notes. Recently, he regaled his younger staffers with tales of the difficulty of obtaining a credit card in the old days. "You went into the bank, and they practically finger-printed you," he recalls. "It was painful." Now, card issuers have figured out how to manage the risk of extending credit to the masses. Consequently, consumers and the merchants that serve them are conditioned to expect a nearly effortless qualification process.

Payment facilitators that can furnish that ease of entry for merchant accounts, while still managing to prevent criminals from obtaining accounts, will succeed, Duncan predicts. Companies like his can help refine the process because they analyze data to understand their payment-facilitator clients and their clients' merchant customers, he claims.

To detect potential criminal activity, ProPay works with third-party partners to authenticate devices, Duncan continues. He also wants to feel comfortable that the data submitted by the account applicant doesn't point to any shady tendencies. Merchants that pass those tests and are approved to open an account then become subject to monitoring, Duncan explains. "It's trying to keep the bad ones from getting set up and then being very vigilant," he notes. The risk department represents a significant portion of a vendor's product offering in payment facilitation, he maintains.

During these first steps of the payment facilitator model, security must come into play. Some payment facilitators have funds deposited to their own accounts and then disperse the funds to their submerchants, says Duncan. Instead, ProPay keeps funds in accounts at major sponsor banks, and the banks pass the money along to the merchants, based on instructions from the payments facilitator, he says. "In the event there's a problem with the merchant, referral partner, or ProPay—from a risk perspective—that money sits with one of the largest financial institutions in the United States."

In addition, security for payment facilitators includes complying with all industry standards, including the PCI Data Security Standard (PCI DSS), Trustwave's Schultz says. "A lot of folks go to the payment facility model thinking compliance and security are not something you have to worry about," he says. "From a legal perspective, that's not the case."

In fact, complying with PCI isn't enough, Schultz maintains. Payment facilitators should embrace payments security so that they can truly become the full-service companies that disrupt the model of ISOs knocking on doors to offer vanilla transaction services, he suggests. "One of our lead QSAs [Qualified Security Assessors] says something funny," he continues. "If you look at a small business that is PCI-compliant, from a security perspective they get a C-minus." PCI compliance represents the bare minimum, Schultz maintains. He describes achieving compliance as somewhat like building the ground floor of a fully secure processing network infrastructure.

As with any payments company, payment facilitators should use tokenization to protect consumers' private data, Duncan notes. His company began providing tokenization services in 1997, long before the payment facilitator model came into being, he says.

Underwriting tools designed to reduce payment facilitators' risk also come into the mix for companies that provide services, says Young. Like all the tools available in the sector, they can be applied in whatever ways suit the client, he says. Sometimes it's a matter of blending tools built by the payment facilitator with those provided by a vendor, he continues.

Payment facilitators should exercise extreme caution and consult with attorneys to avoid classification as money transmitters, Duncan advises. Businesses that fall into that category become subject to state-by-state regulations, he notes.

The card brands handed down the rules for the modern payment facilitator model in July 2011, says Ablowitz. Before that, Visa had defined the "internet payments service provider, or IPSP, but that was a narrower model," he notes.

Today, the payment facilitator approach continues to become increasingly mainstream as processors, acquirers, and the card brands embrace it, Ablowitz says. He likens the sector's history to a freight train plowing ahead since about 2011. Visa's recent announcement concerning the category underscores that burgeoning support, he suggests. Visa announced that payment facilitators no longer need to stand aside and allow banks to take over the relationship when a merchant's annual transaction volume reaches $100,000. The limit has risen to $1 million.

Addressing Risk

The initial spread of the payment facilitator model came with the advent of Square, which offered micro merchants a dongle to swipe cards and onboarded clients with a just a few questions and a minimum of fuss, sources recall. "People who aren't in the payment industry thought the innovation was a little device that could read your credit card," says Young. "That was just the operating system. What they did was introduce payments facilitation to the world. They were the first large-scale, in-market deployment of what we now know as a payment facilitator model."

As payments facilitation becomes more widespread, micro merchants are beginning to demand business services along with payment acceptance, Duncan says. Contractors want software tools that facilitate the bidding process, golf course operators rely on software that helps with scheduling, and retailers depend on automated inventory control, he notes. ISVs that supply the platforms to accomplish such tasks now want to make payments a part of their package, he observes.

The "gamification" of consumer behavior also plays a role in the decisions payment facilitators make, Duncan maintains. Like other consumers, merchants want to play games online for free. They're willing to pay only when an otherwise no-cost game reaches the threshold of the next level, he says. That mentality has led some ISVs to offer their business-function software for free and monetize their products by charging a fee for the payments, he says.

Some payment facilitators want to become full-fledged members of the category by meeting all the requirements to register officially with the card brands, Duncan continues. Many payment facilitators, however, prefer to take on only some of the functions involved and choose to hand off the others to vendors.

The subject of risk often comes up in discussions of the payment facilitator model, with many believing that taking on risk is a primary identifier of the model. But risk becomes negotiable in ProPay's approach, Duncan says. Payment facilitators that are officially registered with the card schemes assume all risk, but unregistered payment facilitators can take on varying degrees of risk and assign the remaining risk to ProPay, he says.

When payment facilitators assume only a portion of the risk, ProPay incorporates its terms and conditions into the merchant agreement, and the merchant knows it is doing business partly with ProPay, Duncan says. When ProPay works with a registered payments facilitator, ProPay can remain invisible to merchants, he notes.

However the risk is apportioned, payment facilitators can use their knowledge of security as a selling point for the system they're offering to merchants, Schultz suggests. He recommends explaining security as part of the full-service consultative approach to dealing with potential clients.

Submerchants also benefit from the payment facilitator model because they enter a relationship only with the payment facilitator, says Young. Under the old model, merchants had to maintain contact with the ISO, the banks, a processor, and possibly a gateway, he says, even though the merchant may not look beyond the ISO relationship. The processor or acquirer enters a relationship with a single company—the payment facilitator—to process payments for multiple merchants, resulting in a cleaner, simpler operation without the risk, he notes.

The payment facilitator model has been tuned to optimize the connection between payments and software, Ablowitz explains. If an ISO wants to sell just a terminal and transaction services to a generic merchant, the payment facilitator mode won't do that much for him, he notes. But if they're tying that terminal to technology, the payments facilitator model will expedite the symbiosis, he claims.

ETA Here To Help

Help has arrived for would-be payment facilitators that are members of ETA in the form of the *ETA Payment Facilitator Guidelines*. The publication, authored last year by Double Diamond Group on behalf of ETA, is intended to help payment facilitators operate within the expectations of regulators and the card schemes, and they include guidance for underwriting, due diligence, and risk management for submerchant accounts.

But not everything that looks like a payment facilitator model from a distance looks that way up close. Some situations vaguely resemble payment facilitator relationships but don't really qualify for the designation under the card brand rules. Uber, for example, operates on the marketplace model because consumers know they are dealing with Uber and will take their complaints to the company instead of approaching the driver, Ablowitz says. In the direct selling model, a company places sales reps in the field, according to Duncan, who says ProPay got a lot of early experience with onboarding very small "merchants" by working in that sector.

Imperfect facsimiles aside, the payment facilitator model appears likely to continue attracting adherents. Not every merchant acquiring relationship will move toward the payment facilitator approach, but the future looks bright for the model, says Young. "Payment facilitators have the wind at their backs," he claims, adding that the model could come to dominate the industry in the United States and around the world, and is certainly here to stay. Ablowitz puts it this way: "Payments are becoming a feature—not a product." ***TT***

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

Seizing the B2B Opportunity

Vertical offers untapped potential to nimble acquirers

By Scott Goldthwaite and Jared Poulson

Electronic payments have made commerce faster, safer, and more convenient for billions of consumers around the world. Consumer payments can be a competitive, crowded market—countless companies, services, and apps are dedicated to helping merchants sell things to end consumers. But there is a vast, largely untapped, market in enabling safer, faster payments for businesses. In 2016, businesses spent $18.5 trillion on business-to-business (B2B) payments, "vastly outstripping the consumer-to-consumer (C2C) and business-to-consumer (B2C) realms," according to *Business Insider*. B2B e-commerce (manufacturing shipments and merchant wholesale, as reported by the U.S. Census Bureau) is growing steadily (increasing nearly 10 percent every year since 2006), with about $5.7 trillion in volume in 2015, according to the more recently available data. The ETA Technology Council surveyed the current state of B2B payments and explored the opportunities available to acquirers that want to break into this vertical.

B2B payments are still largely analog. A Key Bank whitepaper reports that two-thirds of payments made by middle market companies are done via check. For most businesses, paying a supplier typically involves a long invoice trail, phone calls, credit authorizations, and at least a month's wait. But increasingly, businesses are embracing the digital innovation that has transformed consumer payments. This means the market for faster and safer payments solutions that are tailored to the needs of businesses is growing.

Straight Through Processing

The accounts payable (AP) function arguably has the most to gain from embracing digital payments innovations. Within the "invoice to pay" cycle, AP organizations are now moving from a paper-based system to a fully digitized and automated system. Those that upgrade are achieving time and cost savings in their reconciliation and procurement processes, while streamlining other efficiencies in the financial supply chain.

A key component of improving efficiencies for AP departments is straight through processing (STP). STP enables an array of business logic and end-to-end automation that integrates supplier payments into financial and enterprise resource planning (ERP) systems. STP minimizes the complexities involved in matching incoming invoices against purchase orders. STP also allows suppliers to be paid automatically, typically with single-use virtual purchasing cards (more on those later). This automation streamlines the B2B payments processes through predictable validation and three-way matching that offsets some of the manual intervention and exception handling that beleaguers paper check processing. Finally, STP can improve merchant costs as cards typically qualify at commercial card rates.

In a world where you are only as good as your data, a robust STP invoice management system provides value beyond the efficiency of processing invoices electronically. STP generates both a wealth of high-quality business intelligence and the necessary monitoring, reporting, and audit tools to comply with an ever-changing set of regulatory requirements and electronic payment mandates.

The goal of STP is simple: faster business payments through reduced redundancy, errors, and operational risk, with an emphasis on cost savings across the board. However, STP is not limited to B2B payments. It can be used for onboarding of applications (auto loans), cross-selling opportunities, and even data analytics on the transactions between card networks and issuers, allowing account holders greater insight into their purchases.

Electronic Bill Presentment and Payment

As organizations shift more of their business to digital platforms, electronic bill presentment and payment (EBPP) platforms will play an increasingly important role. EBPP already is a core offering of online consumer banking products, whether in the form of biller-direct EBPP, wherein electronic billing is offered directly by the company selling the good or service, or bank-aggregator EBPP, which allows consumers to pay different bills through their bank. However, EBPP has been relatively slow to take off in the B2B realm. Several companies offer electronic invoicing, but few integrate with the ability to pay electronically and automatically.

Offering an EBPP solution can help acquirers and financial institutions differentiate themselves in a competitive market, according to payments provider Aliaswire. As consumers increasingly access the internet through mobile devices (rather than desktop or laptop computers), they demand portable access to online payment portals and the ability to carry out transactions instantaneously, according to a recent study from Transparency Market Research. As more businesses outfit their employees with mobile devices, demand for B2B EBPP is growing as well.

Virtual Purchasing Cards

Virtual purchasing cards, also known as "p-cards," are sometimes referred to as non-distributed cards or electronic accounts payables cards. Virtual purchasing cards don't involve a plastic card and are used to pay for goods and services after an invoice has been received. That is, a virtual card payment is not made at the point of sale. By contrast, a distributed card—which includes travel and entertainment cards and corporate purchase cards—is used for card-present or card-not-present transactions at the point of sale. Some virtual cards are single use (and are deactivated after the transaction has been completed), while others are assigned to a specific vendor account and are used multiple times. Virtual cards can be generated quickly and businesses can specify a dollar limit on each card, making it easy to track and control spending. For example, virtual cards can be issued to employees participating in tuition reimbursement programs. The employer enjoys the security of a single-use card (with a near-term expiration date) for a large transaction that provides an audit trail to the educational institution. Employees appreciate not having to front the money for large educational expenses.

A 2015 RPMG survey found that virtual purchasing cards (referred to in the survey as Electronic Accounts Payable or EAP) are primarily used for goods and services considered too expensive for payment with plastic or distributed purchasing cards (whose average transaction value is $321). The average virtual card transaction value is $4,842. RPMG estimates that overall spending using virtual cards in North America will hit $110 billion by 2019.

Like credit and debit cards for consumers, purchasing cards (whether virtual or plastic) confer a wide range of benefits on the businesses that use them. Purchasing card payments, and particularly virtual card payments, are much faster than payments by check. In fact, a purchasing card transaction is instant, while an automated clearing house (ACH) transaction takes at least one day (for debit; two days for credit), and a check takes at least six days to clear. Additionally, checks are costly to use, with the average check costing up to $10 to cut and process, whereas virtual cards and even ACH are substantially cheaper. The opportunity to pay after the invoice has been received (a float of 45 to 50 days, typically) allows businesses to access more working capital and manage their costs more efficiently, saving more than $200,000 per year by RPMG's estimate. Finally, virtual card purchases are easy to track, enabling businesses to monitor suspicious activity and mitigate fraud risk. With single-use virtual cards, every payment has a unique card number associated with it, which further facilitates reconciliation and account monitoring.

Business Supply Chain

Supplier enablement helps businesses manage their supply chain vendor relationships electronically. This may be as simple as using email to send purchase orders and invoices. An often-overlooked area of savings for B2B merchants is Level 2 and Level 3 data processing. For qualified merchants, the savings on interchange fees for accepting commercial/business credit cards can be significant. To obtain reduced rates from the card networks, merchants must provide additional transaction-level data along with the authorization request. This data varies between the card networks, but typically includes line item info such as product codes, product description, and tax amount. B2B card processing lowers transaction risk by providing more detailed information at the transaction level. A sophisticated supplier enablement solution would allow a business to submit transactions with enhanced data, and allow a business to view and manage all its vendor relationships in a single portal—a place to view and pay invoices, communicate with vendors, and develop billing and delivery schedules.

For acquirers, understanding the supplier's needs and providing the tools and services required to securely process high value transactions is vital to participating in this growing opportunity. Not only are the costs of processing large transactions becoming more competitive relative to traditional methods, but businesses are in a better position to leverage the risk reduction and insights provided by a data-rich electronic transaction. Additionally, for businesses, real-time payments from accepting cards lowers the risk of potentially longer accounts receivable timelines and reduces the labor cost of account auditing that is incurred by traditional payment methods. The costs of accepting card payments, while higher than ACH costs, ultimately compare favorably when measured against the benefits of reducing accounts receivable timelines.

Traditionally, merchant acquiring involved enabling a merchant to accept electronic payments. As innovative new technologies become widely available, acquirers are offering their customers a wide range of services tied to accepting electronic payments—from risk management and fraud prevention to integrated commerce solutions that merge the brick-and-mortar retail experience with e-commerce platforms. Similarly, merchant acquirers can help businesses streamline their supply chain by reducing friction in the payment process. Acquirers can provide purchasing cards, whether virtual or physical, to create consistent records of payment and allow businesses to track and consolidate purchases. A merchant acquirer can at least help a merchant automate its vendor payments if it is on a predictable schedule, or provide EBPP options for vendors that offer biller-direct EBPP. There is much untapped potential in the B2B payments sphere, and acquirers that can adapt to the unique needs of businesses are in a position to thrive in this market. ***TT***

Scott Goldthwaite is SVP of operations at Aliaswire and ETA Technology Council chair. Jared Poulson is chief product and technology officer at Payroc and council co-chair.

ADVERTISERS INDEX

Company	Page	Phone	Web
Authorize.Net	inside cover	425-586-6000	www.authorize.net
eProcessing Network, LLC	9	800-296-4810	www.eprocessingnetwork.com
iPayment	back cover	617-681-6422	www.ipayment.com
Paytrace	cover 3		www.paytrace.com
USA ePay	21	866-812-3729	www.usaepay.com

Guy Berg

As leader of the Accredited Standards Committee X9 Inc. (X9) blockchain study group, Guy Berg will be involved in developing a standardized glossary addressing distributed ledger technology. The initiative kicks off in October, and the project's deliverables will become an ANSI X9 technical report. Here, Berg, who is vice president of the Minneapolis Federal Reserve's payments, standards, and outreach group, discusses the initiative and the need for a common set of terms and definitions for financial services and beyond.

The following has been edited for length and clarity. A fuller edited version of the discussion is available on the *Transaction Trends* website.

What terminology confusion have you witnessed in the financial sector?

This idea came from a work group I've been chairing over the last year, where we were looking at [the] value for standards to support blockchain technology adoption. One of the first things we ran into is that each of us had a different definition for each of the terms. So we spent a number of months trying to work through … vocabulary.

It's really difficult to have a conversation—whether you're a customer talking to a vendor about what they have to offer, or you're a vendor talking to the customer trying to sell them on what you have to offer. If both parties don't understand the terms, you spend a tremendous amount of time just talking about the terms, and you don't get to the meat of the conversation you want to get to.

Think about it: There are a number of different blockchain platforms that are out there. IBM has one. Microsoft has one. Ripple has theirs. They all use slightly different architectures, and they start coming up with their own definitions of terms. Somehow, all of these different platforms need to start using a common vocabulary. If they don't, I think that they're ultimately just hurting themselves in the marketplace, because they're going to end up spending more and more time—or just as much time—in every meeting trying to define each of these terms. I think one of the greatest challenges to blockchain technology overall is the marketplace's understanding of it.

What terms/concepts are problematic?

There are many. The ones that people get the most excited about, often times, are the ones that are most confusing. For instance, people talk about smart contracts. What really is a "smart contract"? If you're talking to people in the legal profession, they may be interpreting it completely different than somebody from the technology side of things. And then the platform providers will have slightly different definitions of how they view and implement a smart contract. ...If I get a group of eight or 10 people in the standards community talking about it, we could be in the conversation for three hours debating [the meaning].

What is the end goal of the technical report? Could it be a definitions standard?

The intent on this new work item would be to develop a set of standardized terms for blockchain technology. That means trying to reach out and talk to all the different entities that are involved in it and look at the terms, how they use them, and come to some form of consensus on a definition that everybody can agree on and move forward with.

Think of all the different functional areas that need to have the same understanding of blockchain terms. There are auditors, regulators, IT groups, and legal that will benefit from having a common reference. Each needs to understand in their terms and from their perspectives. We want to be able to reach out to different entities from different disciplines to try to integrate their perspective into the work. That might be a little bit of a different twist that we're going to try to achieve within this work.

How long will it take?

Standards process is slow. You need to build a consensus, and you need to get the right experts involved in it. You seldom see something that gets done any faster than 12 months. I would hope it would be in a 12- to 15-month timeframe that something could get wrapped up.

[The work group made terminology a top priority], but there are a lot of other areas where I think that this technology could benefit through further standards development. ...Some of it might make more sense to wait another year or year and a half, as the industry evolves a little bit more. An example of that might be the consensus algorithms. Right now, blockchain technology struggles to perform [in a timely manner]. If you're going to get into high-volume payment transactions, you're going to need to perform in sub-second time. The consensus algorithms and processes today just cannot meet that standard of performance, and so there needs to be more innovation. That might be an area where it would make no sense for standards to step in—other than to maybe help identify potential methodologies to stay away from because they may not be considered secure enough. ***TT***

—*Josephine Rossi*

Editor's Note: Professionals from relevant organizations are invited to be part of the technical report initiative. For more information about participating, contact X9 at https://x9.org/contact-x9.