NEW COLUMN: Industry Affairs discusses how ETA and its members are advancing payments innovation PAGE 10

July/August 2018

TRANSACTION trends

THE OFFICIAL PUBLICATION OF THE
ELECTRONIC TRANSACTIONS ASSOCIATION

The Secrets of Social Engineering

Why human weakness is still a looming threat

ALSO INSIDE:

paya

Payments Just Got Better

Merchants are the heart of your business, making their lives easier helps you grow. Paya's payment solutions work in-store, online, or on-the-go. Our secure, reliable platform delivers the business intelligence your merchants need to thrive in a changing marketplace. Partner with Paya today.

Partner Today

www.paya.com

contents

The Official Publication of the Electronic Transactions Association Vol. 23 | No. 4

features

departments

NEW on Page 10!

Transaction Trends introduces Industry Affairs, a new column focused on how ETA and its members are influencing innovation and advancements in payments.

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

ETA CEO Jason Oxman
Vice President, Strategic Partnerships Del Baker Robertson
Director, Communications Laura Hubbard
SVP, Government Relations Scott Talbott
Vice President, Industry Affairs Amy Zirkle
Director, Regulatory Affairs Philip (PJ) Hoffman

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
Sabrina Hicks, Josephine Rossi, Scott Talbott, Christine Umbrell, Kimberly Wheeler, and Amy Zirkle

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 advice and other expert assistance are required, the services of a competent professional should be sought.

Transaction Trends (ISSN 1939-1595) is the official publication, published six times annually, of the Electronic Transactions Association, 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

Introducing the ETA Self-Regulation Program

When ETA was founded 30 years ago, it was the first association to focus on the acquiring side of the payments industry. ETA represented the sales organizations and service providers that sold payments acceptance capabilities to merchants. Established to educate and advocate for ISOs and processors, ETA set the standard for professionalism and proficiency for the acquiring industry. As the sales channel expanded to include independent software vendors (ISVs), payment facilitators, and other service providers, ETA expanded its reach to represent these new entrants into payments.

To fulfill its mandate of fostering industry professionalism, ETA is launching the ETA Self-Regulation Program, a new corporate self-attestation program for the benefit of acquirers, ISOs, and payment facilitators. As new players like payment facilitators, ISVs, and value-added resellers enter the market, acquirers and processors need to feel confident that these new players understand the risks associated with financial services. Further, new entrants must prove to their potential customers and partners that they maintain a high standard of practice. To that end, payments companies that attest to ETA that they have adopted and are utilizing the *ETA's Guidelines on Merchant and ISO Underwriting and Risk Monitoring* and *ETA Payment Facilitator Guidelines* will be designated as participants in ETA's Self-Regulation Program.

The designation indicates to the marketplace that the company subscribes to the voluntary best practices established in those guidelines. The guidelines provide a roadmap for onboarding merchants or third parties and demonstrate how to manage the risk these parties introduce. The guidelines provide recommendations to investigate irregular or suspicious activity by prioritizing security and risk mitigation. They were developed by ETA members to help companies prevent or avoid illegal or fraudulent acts that harm consumers and the payments industry.

Payments technology companies from across the ecosystem—software companies, acquirers, resellers, payment facilitators—will be able to access the program via ETA's website and submit an application, which includes basic due diligence materials. Through the process of attestation, ETA will vet the participants, verify their standings, and publish their participation in the self-regulation program. Although no self-regulatory program can guarantee compliance with the law, this program will help highlight the strength of individual company policies and procedures that follow ETA's guidelines.

Those who successfully complete the program will be provided a certificate and can display the designation on their website and in promotional materials. Additionally, ETA will list its successful participants and communicate the companies' names to federal regulators as having confirmed a commitment to ETA's guidelines. This process will stand to be an important step to further securing and innovating our industry.

In the coming weeks, ETA will launch the program with the support of some of the top acquirers in the industry, and ensure that the program quickly becomes an essential standard for the innovative third parties that are driving payments forward. ETA Self-Regulation Program is the next step in the decades-long journey of ETA, its members, and the payments ecosystem as a whole. As we move forward in this period of innovation, we as an industry must prioritize security and following the rules.

Jason Oxman
CEO
Electronic Transactions Association

Consumers Want Stronger Identity Verification Practices

As high-profile data breaches and privacy incidents continue to make headlines, consumers are more aware and more concerned than ever about the security of their identity information, according to IDology. Fifty-seven percent of American adults surveyed say they are more concerned than they were a year ago that their personal information will be compromised in a data breach, and 83 percent feel extreme to moderate concern that their identities will be used to open fraudulent accounts.

Despite this heightened awareness and growing fear of identity theft, many customers still do not take basic steps to secure their passwords, according to the firm. Forty-four percent of those surveyed admitted that they write their passwords down, while 73 percent rarely change them. Conversely, many consumers say they are open to using more secure authentication methods for online accounts, with 45 percent "extremely or very willing" and 92 percent expressing "some willingness" to do so.

Meanwhile, consumer expectations are higher for the companies that they entrust with their personal identity information. Sixty-seven percent say they "strongly agree" that it is a company's responsibility to protect consumer data. For some consumers, a company's security measures influence where they will do business, with 56 percent reporting that they are "more likely" to choose a financial institution if they know it offers advanced identity verification methods. According to the survey, consumers view biometrics, knowledge-based authentication, and one-time passcodes as the most secure methods of authentication.

The study also found that consumers prioritize ease of use along with assurance that their transactions and identities are secure. When opening an account online, respondents say they place a premium on security (88 percent) and ease (72 percent), with 31 percent of those surveyed reporting that they have abandoned signing up with a business or financial institution because it was too difficult or took too long.

Fast Fact

Most consumers (80 percent) are interested in mobile phone features that allow them to **immediately identify and stop unauthorized credit and debit transactions;** 72 percent value features that provide the ability to instantly see payments made with their credit and debit cards.

Source: "2017 TSYS U.S. Consumer Payment Study," TSYS

Wenjie Dong/iStock/Getty Images

IoT Spending Will Exceed $1 Trillion in 2022

Worldwide technology spending on the Internet of Things (IoT) will reach $1.2 trillion in 2022, according to International Data Corporation (IDC) forecasts. That increase will be realized through an anticipated compound annual growth rate (CAGR) increase of 13.6 percent for IoT spending from 2017 to 2022, as many projects transition from proof of concept into commercial deployments, and organizations continue to invest in rapidly expanding offerings in analytics software, cloud technologies, and business and IT services.

IDC predicts that IoT spending growth will be strongest in the consumer sector, with an anticipated worldwide CAGR of 19 percent, followed closely by the insurance and health-care provider industries. Discrete manufacturing and transportation are expected to be the two largest industries for IoT spending in 2022, as both industries are expected to exceed $150 billion. Meanwhile, vehicle-to-vehicle and vehicle-to-infrastructure solutions will experience the fastest spending growth, with both expecting a 29 percent CAGR over the forecast period, followed by traffic management and connected vehicle security.

Fast Fact

In 2017, 12 percent of U.S. consumers reported that they **did not pay with cash, even once, during the year.** Between 2015 and 2017, the frequency of use of cash remained unchanged.

Source: "The 2016 and 2017 Surveys of Consumer Payment Choice: Summary Results," Federal Reserve Bank of Boston

Wavebreakmedia/iStock/Getty Images

American Consumers Resistant to 'Frictionless' Payments

A new Paysafe research report says consumers are wary of "frictionless" payments—defined as transactions that take place behind the scenes in apps—especially in the United States.

The study surveyed U.S., U.K., Canadian, German, and Austrian consumers about new and traditional payment methods and found that 50 percent of American respondents named fraud as the biggest deterrent to using frictionless payments, with 52 percent reporting concerns about the use of their data.

Twenty-nine percent of Americans have used frictionless payments in apps to pay for goods and services, even though a far greater percentage are aware of the service, according to Paysafe. In addition, only 3 percent of consumers reported using contactless payment methods in the last month.

Why do Americans resist frictionless payments? According to the study, 34 percent of respondents said they are concerned that systems may inadvertently buy things, 24 percent are worried that their spending won't be adequately controlled, and 41 percent said that they are already struggling to keep track of their current subscription-based payments and are hesitant to add more subscriptions that they must monitor.

The study also showed that 65 percent of surveyed consumers think voice-activated systems are not secure, and 69 percent worry that they would be overcharged if they used this type of service. Fifty-seven percent of respondents said they felt that checkout-free stores where smart technologies record the shopping basket and automate payments sound too risky, or they'd need to know more before using them.

Moves & Mergers

Apptizer Inc., an order-ahead storefront technology provider, has appointed **O.B. Rawls IV** to its advisory board. Rawls is currently special advisor to the CEO of Paysafe North America. Previously, Rawls was the president and CEO of iPayment and held leadership roles with First Data, Hypercom, Caredata, Unified Merchant Services, and Bank of America.

BillingTree, a payment technology and services provider, announced it has completed its acquisition of Toledo-based electronic payment firm **Internet Payment Exchange (iPayX)**.

Discover Financial Services President and COO **Roger Hochschild** will succeed **David Nelms** as CEO on October 1, 2018. Nelms will be retiring in 2019.

Global Payments Inc. announced it will acquire AdvancedMD, a could-based software-as-a-service provider, from Marlin Equity Partners.

Payment provider **PayPal Holdings Inc.** has announced it is buying **Hyperwallet,** a company that connects cash networks, card schemes, and mobile money services with domestic ACH networks around the world. **PayPal** also announced that it is buying **Simility,** a fraud prevention specialist. The deal is expected to close in the third quarter.

Paysafe Group, a global provider of end-to-end payment solutions, has completed the acquisition of **iPayment Holdings Inc. (iPayment)** and will be sunsetting the iPayment brand and replacing it with Paysafe's recently relaunched brand. **Todd Linden** has taken the helm as Paysafe's North America CEO of payment processing, and former iPayment President and CEO **O.B. Rawls IV** and former iPayment CFO **Robert Purcell** have both accepted new leadership roles within Paysafe.

TSYS has announced it has acquired **iMobile3**, a Florida company that provides private-labeled, small business solutions and technology services within the payments industry.

VeriFone Systems Inc. has announced that **Michael Pulli** will become its new CEO when the U.S.-based POS terminal manufacturer and payment services provider is acquired by private-equity firm Francisco Partners later this year. Pulli, the former president and CEO of Pace Americas, is currently serving in Francisco Partners' consulting arm.

Created especially for top-tier payments industry leaders and innovators, **this year's ETA Strategic Leadership Forum, October 2-4, in Dana Point, California, promises an unprecedented lineup of prominent CEOs and presidents** of the payments industry. Attendees will hear from leaders who have overseen mergers, acquisitions, and global transitions and can offer relevant and operational insights on the continued evolution of the profession.

Don't miss the following speaker highlights from the three-day event:

Opening Keynote
Tuesday, October 2, 4:15pm
The acquisition of WePay by JP Morgan Chase & Co. resonated loudly through the payments industry as legacy players embrace new emerging forces in the industry. WePay's focus developing APIs to serve platform businesses such as marketplaces, crowdfunding sites, and small businesses presents a nimble model to deliver payments-as-a-service. For Chase, this too brings new opportunities and potential to reach merchants and software providers with ease, speed, and flexibility. Hear from **WePay Co-Founder Bill Clerico** on his vision for the newly merged organization in conversation with **Kim Fitzsimmons, president of merchant services, JP Morgan Chase.**

Morning Keynote
Wednesday, October 3, 9:45am
The Vantiv-Worldpay merger resulted in significant expansion for Vantiv to now reach 146 countries. The deal created the world's largest payment processor, handling a combined $1.5 trillion worth of transactions a year. As a leader at Vantiv and now as **executive chairman and co-CEO of Worldpay, Charles Drucker** has driven transformation and will help plot the course of the future of the payments industry. Drucker and **Royal Cole, executive vice president and head of the North American Region for Worldpay,** will offer their visions of the industry; explain how Drucker sought to leverage partnership opportunities, recognize critical technological trends, and harness implementation; and share the strategic vision for the new Worldpay.

Security as a Strategic Driver
Wednesday, October 3, 10:30am
Security brings critical concerns for the entire ecosystem. Enhancing customer experiences and ensuring robust means for fraud prevention are vital and present strategic options for companies to enhance their value proposition. **Bradley J. Wiskirchen, CEO of Kount; Angela Brown, president and CEO of Moneris; and Ralph Dangelmaier, CEO of BlueSnap,** will address the ways technology is serving the payments ecosystem to maximize security and reduce risk.

Expanding the Reach of Payments—IoT and Connected Cars
Wednesday, October 3, 11:15am
Join **Jon Ziglar, CEO of ParkMobile, and Bisi Boyle, a senior director in Visa's Internet of Things program** for a discussion about the opportunities presented by IoT to enable commerce anywhere. Connected cars that are enabled to support payments provide an opportunity to leverage the utility of cards to any device, anywhere, at any time. Visa has recognized the tremendous opportunities and has been working to bring Visa technology to new vehicles that will integrate with Visa accounts and other advanced auto technologies, including geolocation and 4G cellular connectivity.

Private Equity Panel
Wednesday, October 3, 1:15pm
The pace of merger activity in the payments industry continues to intensify—with upwards of 102 transactions totaling $46 billion in the first half of 2018. Private equity firms have played a major role in driving investment in key players with an eye toward expanding market growth and furthering new opportunities for the payments industry. Led by **Paya President Greg Cohen,** this panel discussion will offer insights from both those sitting in the private equity realm and organizations that have successfully worked in partnership to expand their organizations and align strategic focus.

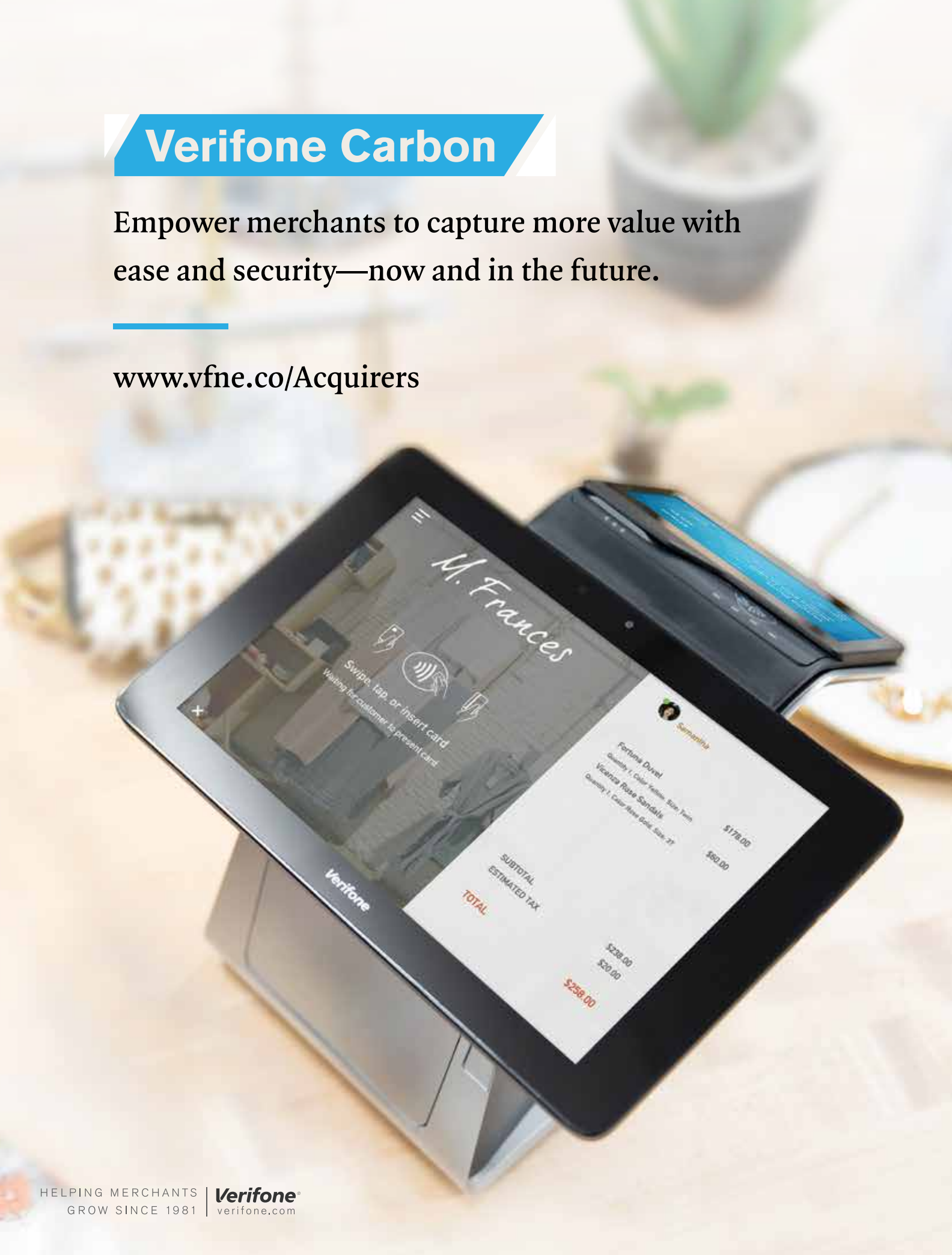
Morning Keynote
Thursday, October 4, 9:30am
As a global leader in fintech products and services, Fiserv brings its solution-defined approach to the payments industry. As the new **president of card services at Fiserv, Kim Crawford Goodman** will offer her unique perspective on the future of the payments industry, having served as an industry leader in major organizations across several markets including payments, software, innovation, and strategic business consulting. Her rich experience brings an important lens through which she will offer remarks addressing the ever-present challenges of changes in card processing, as well as her vision for Fiserv's role in the payments ecosystem.

1. Opening reception at the 2017 ETA Strategic Leadership Forum in Dana Point, California.

Verifone Carbon

Empower merchants to capture more value with ease and security—now and in the future.

www.vfne.co/Acquirers



Developer Central

Enable merchants to do more than just accept payments—with apps that increase business productivity and enhance the consumer experience.

Reflecting and Looking Ahead in 2018

Why it has been a crucial time for payments and policymaking

By Scott Talbott

With the stroke of a pen, public policy can change the business environment. With the calendar year more than half over, it is a good time to reflect on some of the key public policy milestones that have shaped the payments industry and look ahead to those that have the potential to shape it moving forward.

Looking back, we see public policies that have strengthened consumer protections, altered the competitive landscape, and opened up new markets.

Historical Matters

Perhaps two of the most impactful changes to public policy happened nearly 10 years ago. After all, at the time, our economy was in the Great Recession, and policymakers reexamined our political and regulatory framework to deal with the crisis.

Such was the case when Congress passed the Credit Cardholder Bill of Rights law in 2009. The law increased disclosures card holders see on their monthly statement and limited when interest rates could increase. For example, new provisions in the bill required financial institutions to clearly explain to card holders how long it would take to pay off their balance if they only paid the minimum. These types of changes have helped consumers better use credit cards and built further transparency in financial services.

Similarly, sometimes policymakers use policy to shape the business landscape. Arguably the most far-reaching policy change was Sen. Dick Durbin's (D-Illinois) amendment to the Dodd-Frank Act. The amendment, one of the most hotly contested elements of the financial reform bill, set limits on debit interchange rates for large issuers and imposed routing and exclusivity provisions on all debit cards. For better or for worse, the changes this legislation made had a major impact on our industry and will be part of the landscape for many years to come.

Vagabondatheart/iStock/Getty Images

More recent policies have also opened up new markets for the payments industry. Earlier this year, the U.S. Supreme Court invalidated a federal law—the Professional and Amateur Sports Protection Act (PASPA)—that for many years prohibited states from hosting gambling on professional sports within their borders. With PASPA now nullified, there has already been movement in state legislatures—New Jersey, for example—to establish a formal structure for legalized sports betting. As these laws progress, a new business opportunity for the payments industry progresses as well.

Current Advocacy Efforts

Keeping those historical examples of the impact of policymaking in mind, there are issues and political developments currently facing policymakers and the payments industry that ETA is actively engaged in on behalf of our members.

- **One-stop licensing.** One challenge facing a fintech startup is the time and expense of getting licensed in all 50 states, which, given the internet as a medium for conducting business, operating nationwide is a given and a necessity. Getting licensed in all 50 states requires two years and costs millions of dollars—a daunting hurdle for a new company that may have started in a garage. Fortunately, the Office of the Comptroller of Currency is offering a one-stop shop for fintech companies to apply for a national license, which will save time and money and get the fintech's products and services to market quickly.

- **Sandboxes.** Another way key policymakers are helping startups is by providing regulatory sandboxes, which are temporary way stations for a startup to ease into the regulatory environment. As recommended by the U.S. Department of the Treasury, they offer a reduced or limited application of the regulatory structure that recognizes their startup status. As a new business begins to grow and flourish, it moves out of the sandbox and is subjected to the full application of the regulatory requirements. Sandboxes are a great tool that helps encourage startups and allows the economy to enjoy, rather than miss out on, the latest technology.

- **U.S. Supreme Court.** Outside of presidential elections, there is no greater political theater than the presidential

appointment of a justice to serve on the Supreme Court. Unlike Cabinet officials, who can be removed, and members of Congress, who must be elected and re-elected every so often, Supreme Court justices serve for life. That places a tremendous amount of responsibility and authority on the justice. In early July, President Donald Trump nominated Judge Brett Kavanaugh to replace the retiring Justice Anthony Kennedy. The confirmation process by the Senate is likely to be an intense partisan battle.

- **Midterm elections.** On November 6, the entire House of Representatives and one third of the Senate will stand for re-election. Elections are the bedrock of our republic and a constant reminder that our government is of, by, and for the people. In D.C., preparations for the elections have already started. Members of Congress are spending more and more time in their home states or districts, and prognosticators are searching for any hint of how the political winds are blowing. Combine those campaigns with the August recess, and you get a noticeable deceleration of progress on legislative initiatives. It is too early to tell how the elections will go, but with thin margins in both the House and Senate, every vote will count, and the future of the policy landscape will be shaped by those who win the hearts of the electorate.

Across legislative issues of the past, present, and future, it has been and will be crucial for the payments industry to be involved with policymaking. Payments industry professionals are driving innovation—constantly developing and deploying new technologies to help make payments better, faster, and even more secure—and helping the underserved participate in the modern financial ecosystem. As an industry, we must work hand-in-hand with policymakers to keep them informed about the latest cutting-edge products and services, and work toward good public policy that encourages the development and deployment of fintech.

There is no better way to engage with policymakers and help shape policy than to participate in ETA's upcoming events in our nation's capital. On September 5, ETA members can participate in the policymaking process directly at our Payments Fly-In on Capitol Hill. For ETA's government relations team, this is one of our most important tools in the advocacy process, as nothing is more impactful for policymakers than hearing the thoughts and ideas of American citizens leading the payments industry. And on September 6, ETA will bring together policymakers and industry leaders for a forum on fintech policy at TRANSACT Tech D.C. During both events, attendees will hear from and speak with policymakers, leaving D.C. with a deeper understanding of the latest in fintech and how policymakers are thinking about it. As we look toward the future of payments policy, I encourage you to participate in these events and in other ETA advocacy efforts. ***TT***

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

A Leading Role in Innovation

Fintech moves forward through industry collaboration

By Amy Zirkle

As the trade association for the payments technology industry and a hub for the myriad new technologies, products, services, and companies that comprise the evolving market, ETA must have its collective finger on the pulse of the industry if we hope to best serve our members.

So far this year, that has meant understanding the changes in our industry—enablement of new product development through leveraging fintech, emergence of new sales channel entrants and players, evolution of new markets and business models—and working with our base of more than 500 members to grow the payments industry in a time of significant change.

Among our councils, committees, working groups, task forces, and more, ETA has a network of literally thousands of payments professionals—each bringing a unique perspective to the table, on which to build up our industry. This year, our network has been hard at work on two new initiatives that we believe will have a significant impact on the growth of the payments industry.

ETA's Contactless Task Force

Contactless payments feel like magic when you use them—they're quick, they're simple, they're effortless. They're also relatively nonexistent in the United States. Though Barclays issued the first NFC-enabled EMV chipcard nearly a decade ago, the technology has yet to catch on in our American payments ecosystem.

But not for much longer. Earlier this year, ETA announced the formation of our Contactless Payments Task Force. This committee provides an opportunity for a broad survey of stakeholders from across the payments ecosystem to come together and chart a common course toward universal acceptance of contactless payments in the United States.

Chartered by ETA's Board of Directors and chaired jointly by Wells Fargo Merchant Services and Mastercard, the task force includes technology companies, card brands, mobile operators/equipment providers, and financial institutions and actively reaches out to critical players outside of ETA's membership, such as merchant organizations and issuing banks.

To achieve the momentum for boosting contactless card and mobile payment adoption in the United States, the Contactless Task Force will be striving for collaboration. To us, key components of collaboration include articulating agreed upon basic principles that guide development, considering relevant industry incentives, determining a potential roadmap to further goals, and working with key standards organizations (such as EMVCo) to consider where opportunities exist for collaboration.

metamorworks/iStock/Getty Images

The Contactless Task Force met at TRANSACT this year and regularly holds calls. As the task force's work continues, we will be focusing on building out a standard course for payments companies that establishes a reasonable amount of consistency for consumers and merchants alike. The task force also is working to develop additional tools to drive merchant awareness and promote strategies to boost adoption by maximizing the unique value proposition of contactless payments. Other top priorities include developing strategies for merchant education, equipment evaluation and enablement, troubleshooting, and support.

ETA's Contactless Task Force will meet next at our Strategic Leadership Forum (SLF), October 2-4, in Dana Point, California. SLF will surely provide a very useful forum for all of payment's stakeholders and help us maximize the positive impacts of contactless payments technology.

ETA's Payment Facilitator Committee

Payment facilitators have driven change in our industry, and the business model is growing its presence, bringing new players to an already competitive marketplace in payments technology. In fact, ETA's membership includes many companies working in the payment facilitator space and other software innovators. Our members in the traditional sales channel and merchant acquiring spaces also have taken a notable interest in the role that payment facilitators play as they seek out new partnerships and broaden their reach to new merchants.

ETA has convened a Payment Facilitator Committee, made up of a wide cross section of players. The committee includes payment facilitators as well as other key segments, including acquirers, processors, card networks, and more.

The continuing growth of the payment facilitator presence in the payments ecosystem brings greater opportunities for ETA to help develop industry information and guidance for both payment facilitators new to the payments ecosystem as well as current players in the market who want to gain a better understanding of key operational approaches tied to payment facilitation. For 2018, the ETA Payment Facilitator Committee has taken on some new and exciting projects to help further examine, define, and engage with the growing presence of these new players in our payments ecosystem.

The first project concerns understanding basic terminology, which is fundamental to the growing conversation surrounding payment facilitators. For example, some confusion exists around use of the term "payment facilitator" and the additional language that speaks to how these players operate in the market. That's why ETA's Payment Facilitator Committee is currently working with a broad range of stakeholders to reconcile and identify core terms that address this segment of the market and develop one glossary that will serve as the reference point across the payments ecosystem.

With the completion of the glossary, our goal is to elevate the conversation by enabling easy discussion of the issues and boosting communication. Ultimately, elevating the conversation will be important to promoting collaboration and competition in the marketplace.

The Payment Facilitators Committee also is hard at work on revising the *ETA Payment Facilitator Guidelines*. The guidelines were developed as a tool to aid payment facilitators in their underwriting and risk management program.

Underwriting is a critical piece of the payments ecosystem on which so much is based. These revised guidelines will consider cutting-edge fintech innovations and the pace of change in the industry to give clear guidance to payment facilitator entrants on how to best structure their payments business. Keeping the guidelines timely means that further trust and a basis of understanding across the marketplace will let traditional players and new entrants understand fully the role and responsibility tied to the payment facilitator space.

ETA Members Lead the Way

Through these initiatives—and many others in ETA's industry affairs work—our members play a definitive role in the next generation of payments technology. Whether it's leadership in contactless payments, payment facilitators, or other industry issues emerging on the horizon, the collaboration between ETA's dedicated volunteer leaders helps us achieve our mission of ensuring a rich and growing payments ecosystem. As we look forward to the second half of this year—to the great meetings we have planned through TRANSACT Tech D.C. and the Strategic Leadership Forum, to the work we have done and the work we need to do—we at ETA are truly excited to see the positive outcomes our members will help us achieve. ***TT***

Amy Zirkle is vice president of industry affairs at ETA. Reach her at azirkle@electran.org.

The Secrets of Social Engineering

Forget the Nigerian Prince Scam. More sophisticated attacks that exploit human vulnerabilities and target payments are on the rise

By Christine Umbrell

We've all heard the stories in the news about cyberattacks enabled by unwitting consumers: fraudsters hacking into individuals' email accounts and sending messages to their contacts requesting money; consumers providing payment information to phony websites; cybercriminals pretending to be relatives "in urgent need of funds." These are just a few examples of social engineering fraud, which is a growing problem for consumers and companies—and, by extension, payments professionals—as scam artists evolve into increasingly sophisticated criminals and their attacks become more targeted.

"Social engineering fraud" can come in many forms, with the most problematic for payments professionals being virtual attacks, carried out online. These often involve "phishing" schemes, such as initiatives where fraudsters send out mass emails containing fraudulent links to a wide range of recipients, or "spearphishing" schemes that have a higher degree of sophistication and are targeted to specific individuals or companies.

"Social engineering is the manipulation of a person to get information or have them perform some type of act they wouldn't otherwise perform," explains Ryan Jones, managing principal, labs, at Coalfire. Hackers use phishing and other social engineering methods to target organizations with legitimate-looking emails, social media messages, and phone calls that trick users into providing confidential data, such as credit card numbers, Social Security numbers, account numbers, or passwords, according to the PCI Security Standards Council (SSC). Most commonly, hackers use phony emails, containing malicious software that could infect computers and systems, or that contain links to lookalike sites. Fraudsters also exploit website and software vulnerabilities and compromise credentials to gain remote access to a network, by using unauthorized usernames and passwords.

Over the past few years, social engineering has been the main entry point for the majority of breaches, according to Jones. "They're easy to do, they don't require a lot of technical knowledge, and they're an easy way [for criminals] to get a foothold

MR1805/iStock/Getty Images

into the internal networks of a company," he says.

"When they're successful, phishing attempts can have a significant impact on you personally, as well as on your workplace," explains Mark Carl, CEO of ControlScan. "Spearphishing attempts can be very targeted and very sophisticated, and were the most expensive—and successful—types of attacks last year."

Kaspersky Labs detected more than 46.5 million general phishing attempts in the second quarter of 2017 alone, and while the overall number of spam incidents decreased in 2017, phishing attacks increased. "These tend to be the most costly because the attacker is often looking for something that has value, such as payment card data [from which they can] print their own cards for use online," says Carl. "They may also be looking to install ransomware."

Exploiting Vulnerabilities

Last year, social engineering attacks were utilized in 43 percent of all breaches in a broad dataset examined by Verizon. "Almost all phishing attacks that led to a breach were followed with some form of malware, and 28 percent of phishing breaches were targeted," according to the "2017 Verizon Data Breach Investigations Report." Phishing was the most common social tactic in the dataset (93 percent of social incidents).

These numbers match what Jones is seeing at Coalfire. His company's research revealed that midsized companies are at greatest risk of social engineering penetration—despite being more secure overall. Smaller organizations tend to be more intimate environments, where individuals are more in tune with the operation of the business and employers personally promote awareness, according to "Coalfire's Penetration Risk Report, 2018." Conversely, large businesses benefit from having "seen it all," by nature of having such a large staff and frequently engaging in strictly administered, recurring, and regularly audited security training and awareness programs. But midsized organizations, according to the research, "are stuck being too big to provide staff with a natural awareness of company operations, yet too small to have assembled formal training, awareness, and draconian email controls. This leaves them susceptible to the broadest range of social attacks."

Cybercriminals themselves have evolved from individuals or

small groups into large, organized criminal entities, according to Michael Aminzade, vice president of global compliance and risk services for Trustwave. "They are well-funded," he says. "We have been able to identify specific large organizations and have found that they do feasibility and ROI studies" to determine whom to target.

Robert Capps, vice president and authentication strategist at NuData Security, offers rationale for the uptick in social engineering attacks: "Fraudsters are awash in stolen data—there are more stolen data records out there than there are human beings. So now [criminals] need to figure out what is relevant data," says Capps. Phishing, and spearphishing in particular, help criminals do that.

Payments professionals should understand that retail spaces, which typically have high staff turnover and low margins, are especially susceptible to social engineering attacks. "It's hard to get employees to a level [where they can successfully serve] as a first line of defense," says Jones. "They usually have firewalls and conduct limited testing to protect themselves at the perimeter, but hackers are able to get to the systems on the inside. Just one person who responds to spearphishing or otherwise compromises the system is needed" to infect a system.

In fact, Trustwave Spiderlabs investigated malicious data breaches affecting thousands of locations in 21 countries as part of its "2018 Trustwave Global Security Report" and found the largest single share of "incidents" involved the retail industry (nearly 17 percent), followed by finance and insurance (13 percent), and the hospitality industry (nearly 12 percent). Half of the incidents involved corporate and internal networks, followed by e-commerce environments, at 30 percent. Incidents affecting POS systems accounted for 20 percent of the total.

"Threat actors" targeted payment card data in the majority of incidents, with magnetic-stripe data comprising 23 percent of incidents and card-not-present data comprising 20 percent, according to Trustwave. In addition, 47 percent of the POS system compromises were accomplished via phishing and other social engineering attacks. "These can happen when administrators don't properly segregate the cardholder data environment from the rest of the network," the report states. The hotel and restaurant sectors were especially vulnerable to these types of attacks.

Trustwave also reported that remote access attacks were the second most common method of compromise at the point of sale. "Often, the attacker gained remote access to multiple locations by obtaining service-provider remote access credentials, either by compromising the service-provider network (and thus VPNs) or by simply obtaining default passwords in cases where remote access tools were internet accessible," the report states. "The human factor is still the highest source of weakness for corporate environments, with phishing contributing to more than half of such compromises."

In addition to compromises stemming from fraudulent email, the retail industry is seeing more attacks that draw customers to copycat merchant websites. Cybercriminals are using international typographical characters to create a website URL that's very similar to a legitimate website, explains Capps.

A new report from Farsight Security found an increasing prevalence of Internationalized Domain Name (IDN) lookalike names, or homographs. IDNs enable a multilingual internet by allowing users to register and use domain names in different languages. Because IDN homographs are easy to register and often go undetected by traditional security solutions, the lookalike domains are increasingly being used to commit phishing and other malicious activities against unsuspecting consumers who mistakenly believe they are on legitimate websites, according to the Farsight research.

Capps notes that while phishing scams and the use of internationalized characters in domain names are not new, "the resurgence of embedding foreign characters with subtle differentiations to English language ones to draw customers to phishing sites is an interesting twist. It shows that hackers are constantly evolving and changing tactics to lure customers into surrendering their personal and payment data—even if those techniques are not new or novel."

Prevention and Response

Many organizations are adjusting their security practices and working with partners in prevention strategies, but keeping pace with fraudsters' constantly evolving attack practices can be challenging. "We've done a lot of good in educating people on what links [are OK] to click, and what calls to take," says Aminzade. While new security technologies help prevent and minimize attacks, "criminals also realize what areas are hard to attack—for example, areas that have shifted to EMV," and concentrate their efforts in alternate, more vulnerable areas.

"It's very difficult to prevent these types of attacks," concedes Jones. "There's no silver bullet for security—social engineering or otherwise. But you have to train employees, make sure they know who to report compromises to. And it's important that everyone use strong passwords and apply patches internally as well as externally."

The PCI SSC offers several recommendations to decrease the likelihood of an attack causing damage. Companies should reduce unwanted email traffic by installing and maintaining basic security protections, such as firewalls, antimalware software, and email filters. In terms of website and software security, companies should separate and update computers and software—for example, use basic security tools and keep computers used for social media sites, email, and browsing separate from computers used for processing financial transactions. And everyone should be practicing good password hygiene, updating strong passwords regularly, and implementing two-factor authentication.

Sources caution that PCI compliance is only a minimum standard. "Merchants need to be conducting risk assessments and more sophisticated testing, and adhere to stricter standards as they are developed," Aminzade says. "Compliance standards will always fall behind [the capabilities of criminals] so merchants need to take a 'security first' approach."

"Social engineering is going to be a threat to any business," Carl says. "Anywhere you have a connected employee, you are susceptible." He recommends limiting access to IT systems so only those who truly need it have access to data. He also suggests training employees not to click on suspicious links. In addition, "have a security system in place 24/7, so if a PC gets infected with malware, endpoint security can take it offline immediately," suggests Carl.

Point-to-point encryption (P2PE) surrounding payments

Partnerships Needed

Given the countless methodologies cybercriminals are now using to exploit human weaknesses to steal data, it's important for payments professionals to work with partners and merchants to ensure everyone is on the lookout for social engineering schemes, say experts. Merchants should understand that even if attacks themselves aren't too costly, the response and recovery costs could be much higher.

Mark Carl, CEO of ControlScan, points to an incident at Erie County Medical Center (ECMC) in Buffalo, where an April 2017 ransomware attack on 6,000 computers demanding a $30,000 ransom actually cost the health-care provider nearly $10 million in recovery costs. Hackers had gained access to a server after scanning the Internet for potential victims with port 3389 open and Remote Desktop Protocol (RDP) exposed. They then forced an RDP connection using a relatively easy default password, according to reports, and infected the system with SamSam ransomware, including a ransom note for 24 Bitcoins (roughly $30,000).

After careful evaluation, ECMC decided not to pay the ransom—seeking to maintain the integrity of its systems, and not trusting the hackers to deliver decryption keys—and shut down all computer systems for several weeks, with staff turning to written patient notes until patient electronic health records were fully restored four weeks later. Three months after the attack, roughly $5 million had been spent on computer, hardware, and assistance needed in the response, plus another $5 million in estimated business losses and increased expenses.

is critical, sources agree. "You need to de-value the data coming in," says Carl. "P2PE must be applied at the point of interaction, immediately when the card or chip is read." He cautions organizations to remember that even if attackers can't get access to payment card data, companies still may be susceptible to ransomware.

Aminzade also urges the retail sector to adopt P2PE systems. And he suggests that payments professionals survey the evolving landscape; actively work with QSA and security partners to stay up on the latest happenings; check the blogs of security experts and the card brands; undergo relevant training; and understand how payments are developing—particularly mobile and contactless payments.

He further emphasizes that securing payments should involve a comprehensive approach. "You can't just focus on payments; you need to look at the identity of the person making a payment, and not just the card," Aminzade says. "You need to really understand personal data regulations, and expand your focus area into protecting personal data."

Capps suggests that all parties associated with transactions, and anyone with a loss budget, focus on "tying the individual at the keyboard—the consumer—with the rightful owner of the account data," and ensure appropriate credentials are provided. This will devalue stolen data, eventually reducing the incidents of phishing and data breach.

Some merchants and financial institutions are responding by moving past the user's personally identifiable information as a way to authenticate them—as this could have been stolen by phishing, for instance—and incorporating multilayered solutions with passive biometrics and behavioral analytics, says Capps. "These technologies thwart the reuse of data by fraudsters and, instead, verify users based on their behavioral information. The hundreds of subtle nuances in customer behavior—together with many other factors such as device identity—create a dynamic user profile that bad actors can't mimic."

Many companies offer services designed to help protect data and prevent social engineering attacks. ControlScan, for example, has an Active Monitoring Services Division that offers managed detection and response services. Its services are designed for enterprise security as well as retail.

Aminzade notes that companies that leverage Trustwave's security systems, or similar systems, have an advantage because they receive warnings of attacks being carried out on other entities. "If we see an attack starting to happen in a certain vertical, we can create targeted defenses for other merchants in that vertical," says Aminzade.

Ongoing Vigilance

Just as security technology is getting more sophisticated, so, too, are the attacks, sources agree. "We expect more phishing attacks will become spearphishing—more targeted," in the future, says Carl. "Humans will always be the weakest link."

Jones predicts that today's "simple" phishing attacks will become much more intricate tomorrow. He speculates that criminals will conduct in-depth research on individuals at the companies they are targeting, perhaps learning details about their hobbies and their friends, to "create an even more targeted attack."

Capps believes the coming months will bring "more attacks on consumers." He urges payments professionals to "be aware of the latest trends, and adapt businesses to be more resilient to attacks." To prepare for social engineering attacks, he suggests that payments professionals aid merchants in looking at the competitors in their space to evaluate how similar companies are being compromised. "The attackers usually start with the biggest companies, then as those companies protect themselves, they move down to the smaller companies who are not likely to be prepared," Capps explains.

"These types of attacks are not going away," says Jones. It's time to "stop looking at employees just as the weakest link and start thinking of them as the first line of defense" to help protect companies, consumers, and payments systems. ***TT***

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

Security NOW

What's top of mind at several security firms

By Kimberly Wheeler

Consumers expect an electronic payment experience that is convenient, easy, fast, and, above all, safe. Payments professionals are under pressure to deliver enhanced, protected payment experiences in a sophisticated and evolving landscape of security threats. These demands create technical challenges for merchants, pushing them to find a way to secure not only their payment processes but also every stage of the payment lifecycle, from the moment consumers first visit the merchant's website or store to the time of checkout and beyond.

One of the most crucial aspects of addressing these challenges is simply staying informed of the shifting threats facing the industry, say experts. To that end, we asked several to offer their perspectives on key issues and pressing fraud trends across the market, as well as the solutions available to mitigate them.

Trends: 'Industrialization' of fraud and insufficient security measures

As businesses scramble to fend off evolving security threats to card-not-present transactions, the fraudsters perpetrating them are only getting more sophisticated and more organized, and that in itself is a concerning trend, notes Don Bush, vice president of marketing at Kount, a fraud detection and prevention service.

"Data breaches used to be kind of an anomaly. But over the past three or four years, they have become commonplace—so common that some 2 billion records have been compromised," he says. "When you consider that only 3.5 billion people on the planet have regular internet access, that's pretty dramatic."

Calling it the "industrialization of fraud," Bush explains the fraud market has become increasingly easy for the average criminal to enter, with few barriers, if any. Stolen data and the tools to use it are readily available, easily obtained, and inexpensive to use. In addition, fraudsters are becoming increasingly sophisticated in how they profit from their stolen data and goods, using them to develop their own businesses.

"Within the fraud market, all of these submarkets are developing," he says. "We're seeing fraud groups starting to specialize. If I'm a fraudster who specializes in shoes, I know how much I can charge, shipping, what the market will bear, distribution points, what websites to set up or go to to sell what I steal. Ridiculous as it sounds, it's true. Fraudsters can sell everything from PayPal accounts to nutritional supplements because they have good data, know the market, and know how to turn it into cash."

Segments of the market going through a digital transformation are particularly vulnerable, Bush suggests, because they often don't anticipate the volume and diversity of threats that they are now exposed to in the card-not-present (CNP) environment. Merchants transitioning to digital platforms may mistakenly take a similar security approach to CNP that they would with card-present transactions. To make matters worse, many merchants designate their in-store loss prevention managers to oversee security for their digital platforms, even though those personnel often lack the necessary training, experience, and expertise.

"It's more naive than negligent—they're naive to the sophistication of fraudsters, how they can infiltrate an app, and don't necessarily understand that, with a card-not-present transaction, different rules apply, different liability," Bush explains. "With in-store purchases, liability is on the bank as the point of sale, but when you're online, the liability is on the merchant. And when you are inexperienced at dealing with fraud, it gives criminals a whole new avenue of opportunity."

While data breaches aren't going away, Bush says businesses can protect themselves by employing more thorough fraud mitigation tools—asking for card verification value or address verification just isn't enough. He recommends that merchants

first check with their payment processor to identify tools or services the processor has vetted and offers to its clients as part of its service. Another option is to obtain a complete platform fraud system that combines various security screening and fraud mitigation tools into one platform, making it easier to use and reducing the need for technical support.

"A complete platform will take all these different screening tools and feed their results into a sophisticated machine-learning algorithm that will tell you whether a transaction is high-risk or legitimate," Bush says. "That type of assistance happening in milliseconds gives the merchant a chance against these fraudsters."

Regardless of the type of fraud system a business is using, Bush says it is essential for merchants to conduct a fraud audit at least once a year.

"Merchants will change payment types, processors, might go to new countries, or offer new products, and, every time they make a change, it's a new opportunity for fraudsters to infiltrate and make trouble," Bush warns. "Do a fraud audit at least annually, maybe every six months or even quarterly. Run the numbers that you have available, the benchmarks that tell you whether you are doing better or worse than before—your manual review rate, your false positive rate, acceptance rate, chargeback rate."

Trends: Internal fraud and merchandise pick-ups

While many merchants tend to focus on the fraudster threats from outside of their organizations, it is equally important to look inside the business, says Monica Eaton-Cardone, owner, co-founder, and chief operating officer of Chargebacks911, a company dedicated to mitigating chargeback risk and eliminating chargeback fraud.

Chargebacks911 has seen a concerning trend of internal fraud among its merchant clients, says Eaton-Cardone. This type of threat is posed by current or former employees and affiliates, such as contractors, who have access to a merchant's network or data. It can involve anything from stealing customer account information to installing harmful scripts on a merchant's system.

"We are seeing more prevalent instances of collusion and internal and affiliate fraud," she explains. "Specifically, we see this happening more and more often when businesses are going through seasonal growth around October—increasing the manual review team, increasing tech support, increasing staff across the board, and using more affiliates."

While the number of incidents may be increasing, the speed with which they are identified is not keeping pace—incidents of internal fraud can often take as long as 18 months to detect. Eaton-Cardone says the key to detecting internal fraud is a multifaceted approach to protection that involves regular reviews, not just of transactions but specifically of declines. "Merchants need to take a multilayered approach to cybersecurity. It's absolutely crucial," she suggests. "Many companies become victimized because they have one fraud solution in place, and it's just not enough."

Manual review is one layer that Eaton-Cardone recommends companies build into their fraud mitigation approach. "There are still patterns that only the human eye will detect. Take a sampling of all decline data and give that to a human review team that can look for bizarre trends. More intelligence and understanding can be gained from analyzing decline patterns than from just looking at approved transactions."

Another threat that Eaton-Cardone notes is on the rise is a relatively little-discussed scheme that involves merchandise pick-ups at stores.

Most major brands and retailers allow customers to order items online and arrange to pick them up at a local store. The problem is that many merchants do not require any type of identity verification at pick-up. Customers may be asked to show a receipt, but they are rarely required to provide a photo ID or to sign anything to pick up their item. Meanwhile, the companies don't become aware that store pick-up fraud has taken place until two to three months afterward when they receive a chargeback for the item.

"Store pick-up fraud has grown by 26 percent with the merchants we serve," Eaton-Cardone says. "Invariably, the fraudster uses a stolen credit card, just a simple AVS certification and Zip code, orders the item, then they go pick it up and sell it on Ebay, and no one ever gets caught. This is a massive loophole that affects every client that we have in big-box retail."

While the problem is serious, the solution is simple, says Eaton-Cardone. Merchants can protect themselves and consumers simply by changing their store policies to require customers to show photo ID when they pick items up at the store. And again, she notes, reviewing revenue declines can help identify trends like store pick-up fraud.

"Study your chargeback data," Eaton-Cardone stresses. "Chargeback analysis has the richest data because it tells you all of your mistakes. Most of us learn our lessons from our mistakes. The gold mine in your business is the data in the chargebacks."

Trend: Ransomware

Although it is imperative that businesses be on the lookout for new security threats and trends, it is also important to keep an eye on those threats that have been around for a while, and even those that may seem dormant, says David Ellis, senior vice president of forensic investigation at SecurityMetrics.

Ransomware is one of the top security concerns for the electronic payments industry, but many merchants may not even consider it a threat anymore. Still, these malware attacks persist and continue to block users' access to their own systems, causing not only loss of revenue, time, and data but also consumer confidence.

Ransomware attacks are not a rare scenario and, according to Ellis, they are every bit as damaging as other fraud methods garnering more attention and action. He describes a recent ransomware attack on a SecurityMetrics customer with more than 1,000 locations, in which the company focused on securing its cardholder data environment but lowered its defenses in other parts of its network.

"They got hacked outside of their [cardholder data environment], but the hackers had built a robust ransomware and it locked up all of their systems," he recalls. "For several days, they could not do anything. They couldn't process card transactions or even send emails. It brought them to their knees because the card data environment itself wasn't targeted for data, their overall structure was. It completely impacted their business."

Ellis explains that ransomware attacks are most often delivered to a merchant's system through employee emails. Some phishing attempts are obvious and unlikely to fool employees, he says, but those attempts are often meant to distract employees and lower their defenses so that they won't recognize more sophisticated attempts.

"The fraudsters are creating a veil that has someone thinking, 'That's what phishing looks like, these blatantly obvious attempts that no one is falling for,'" he explains. "But, the reality is that fraudsters have gotten so much better about disguising phishing emails with malicious payloads attached to them … and are now even able to pose as a person's bank."

Defending against ransomware, Ellis says, is largely about educating employees to look for and recognize phishing emails, no matter how sophisticated. However, to detect ransomware and other breaches, merchants also need to employ regular file integrity monitoring—not just a program to monitor the company's systems but a person to monitor the program.

"Not every attack is going to throw up red flags immediately," he says. "Some breaches have taken as long as five to six months before someone caught on because, even though the company had ample, terrific security logs and the early warning systems and file monitoring systems were throwing out alerts, nobody was watching."

Ellis encourages businesses to consider designating an employee who has the specific responsibility to monitor daily security logs and scan for anomalies. The designated employee should also be able to receive phone notifications when security systems detect unusual or suspicious activity and should know how to recognize and respond to both false positives and real threats.

"When a merchant can identify a breach right away, they're able to secure the systems and lock out the hackers within hours or days," Ellis says. "Imagine being able to catch it in the first few days versus once it's been going on for months or even years."

Trends: Account takeovers and loyalty program abuse

Among many other advances in fraud activity, the shift from simple card information theft to full account takeover is a concern, says Vered Gottesman, vice president of marketing at Forter, an e-commerce fraud prevention company.

"Fraudsters are not just looking at transactions anymore," Gottesman says. "Instead, they've moved upstream and identified more sophisticated ways to attack. Account takeover is an ever-increasing form of fraud. They don't just steal the customer's card information—now, they conduct transactions posing as the customer."

With account takeover, fraudsters access data that can be used right at the point of sale to obtain products and services through the victim's account. Speed of detection often depends on how vigilantly the victim monitors his or her account, as the transactions often don't raise red flags for less accurate fraud mitigation tools that rely on human reviewers to approve or deny online payments.

More specifically, Gottesman says incidents of account takeover fraud involving loyalty program abuse have recently spiked. Fraudsters hack user accounts and deplete loyalty or reward points without the user noticing. Many merchants design their loyalty programs for ease of use rather than security, which often means that users aren't required to enter a form of payment or other information that would verify their identity. Once they obtain access to a victim's loyalty program account, fraudsters can use the payment and personal data displayed in the account to make purchases, accrue points, then redeem them before the fraud is detected.

Gottesman says these trends reflect a perfect storm that makes it easier for fraudsters to access account information and pose as the consumer, perpetrating crimes undetected.

"What you have is all these different circumstances emerging at the same time," she explains. "You have the huge increase in online fraud, the abundance of data available, the ability for fraudsters to specialize and become automated, the commoditized hardware, and the really high—and increasing—cost to merchants."

To combat these fraud-enhancing factors, Gottesman recommends that merchants structure their organizations in a way that emphasizes fraud as something that impacts the whole business, educating employees from every department that could be affected to improve their awareness of, and vigilance for, emerging trends in fraud.

She also recommends employing a customized fraud protection service: "In the face of rising threats and the complexity of the fraud that is emerging, you just can't use a one-size-fits-all approach," she says. "Every business is different—every business has a unique risk profile and different needs. Businesses shouldn't take a simplified or overly standard approach to fraud protection." ***TT***

Kimberly Wheeler is a contributing writer to Transaction Trends.

Beyond the Point.

ETA SLF | DANA POINT, CA | OCTOBER 2-4

KEY STRATEGIC UPDATES

- **US Contactless Task Force:** Hear from key leaders
- **Payment Facilitator Ecosystem:** New initiatives, opportunities and guidelines
- **International Payments:** Policy updates and business opportunities

eta STRATEGIC LEADERSHIP FORUM

Register today at **ETASLF.COM**

Which Way, Contactless?

Navigating the direction of tap-and-go technology in the United States

By Josephine Rossi

Don't call it a comeback. U.S. contactless payments have been around for years—since the mid 2000s, in fact. But renewed conversations initiated by security upgrades, innovative form factors, and high-profile marketing efforts have the payments space wondering if the tap-and-go technology will finally take hold.

"When compared to countries like the U.K. and Australia, the United States is still in the early stages of adoption, but we definitely see the potential for merchants to be ready and willing," says Liz Ryan, executive vice president, Wells Fargo Merchant Services, and chair of ETA's Contactless Task Force, who cites the number of NFC-enabled POS devices deployed and "complimentary inroads" via mobile wallets and wearables as momentum. In addition, with the growth of NFC-enabled ATMs, "we see consumers leveraging contactless activity more broadly in their everyday lives, and this activity will bring more familiarity and, consequently, adoption," she says.

Indeed, contactless is now based on EMV standards, and most new POS devices are able to conduct contactless transactions, according to the Secure Technology Alliance, which says that more than 95 percent of new terminals shipped are contactless capable.

Other industry data and analysis also point to a ripe environment: One of the most recent studies comes from global management consulting firm A.T. Kearney, which asserts 70 percent of U.S. merchant terminals have the necessary hardware for contactless, and 48 percent of face-to-face transactions are happening at contactless-enabled locations. (For its part, Visa announced earlier this year that it expects 50 percent of U.S. in-person transactions will occur "at contactless-enabled merchant locations" by the end of 2018. Meanwhile, the U.S. Payment Forum reports data from Mastercard indicating nearly 800,000 U.S. merchant locations were already contactless-enabled as of the fourth quarter of 2017.)

While he won't call it a "boom," Paul Kobos, senior vice president of banking and payments for Gemalto in North America, says issuers are starting to "show genuine interest" in contactless, too. "Initially, we're seeing reissuance cycles of cards that are contactless-enabled based on segmentation of customers."

Specific portfolios, such as high-volume transacting customers and frequent travelers, will be the first to receive contactless cards, according to Kobos. He predicts that issuance and consumer adoption rates will take off after users are able to experience the technology for themselves. "It's tough to say exactly how quickly that will transpire, but we feel strongly that it will happen over the next couple of years," he says.

Although issuers such as Capital One and American Express have already begun introducing the new cards, only 5 percent of cards today are contactless, according to the Secure Technology Alliance. Ryan says Wells Fargo is "evaluating the marketplace to identify when to offer dual-interface on other card products." It currently offers dual-interface credit cards upon request to Signature and Platinum customers.

TRANSACTION TRENDING
THE OFFICAL PODCAST OF THE ELECTRONIC TRANSACTIONS ASSOCIATION

Listen to Wells Fargo's Liz Ryan discuss contactless and the new ETA task force on the 12th episode of ETA's podcast, *Transaction Trending*. Visit www.transactiontrends.com and subscribe to *Transaction Trending* on Apple Podcasts, Google Play Music, SoundCloud, or Stitcher.

cheekylorns/iStock/Getty Images

Accelerating Movement

Despite the positive indicators, sources say a lot of work is needed before contactless will become popular in the United States. Blame it on the complex and ever-evolving payments infrastructure, lack of consumer and merchant awareness and incentive, software and hardware certification, and more, but the massive growth that's occurring in other countries may not become a reality stateside.

Comparing contactless to the recent EMV chip implementation isn't an equivalent comparison, says Kevin Morrison, senior analyst on Aite's retail banking and payments team, who is conducting preliminary research on the topic. Consumer protection was the "linchpin" that drove implementation and acceptance of EMV, he says. "We haven't seen something of that magnitude drive the need for [contactless] technology to be implemented from a public opinion standpoint or from a political standpoint."

Speed and ease of payment are two incentives for contactless adoption, according to Matt Donnelly, vice president of solutions and finance at FreedomPay. His company works in niche verticals such as contract food service in sports stadiums, where merchants have not yet adopted EMV due to transaction lag time. "Even two seconds … is too slow for them," he says. With transaction amounts typically less than $25, there's little reason to make the switch from a liability standpoint, so contactless is "the only way they want to move forward."

The public transit sector offers another "proving ground for the consumer use case that could give contactless the boost it needs to take off en masse," says Kobos. Because the majority of people who use public transportation typically use the same payment method on a daily basis, behavior can quickly become habit and encourage tap-and-go use for other transactions. "Contactless public transit payment systems [are] already implemented or being designed in major metro areas including Manhattan, Chicago, Toronto, Vancouver, and even midsize markets like Portland and Salt Lake City," he says.

Anytime Visa puts marketing dollars behind an initiative, consumers take notice, Donnelly adds, citing the card brand's Super Bowl ad spots in February. Still, he says it's incumbent on payments professionals to come together to educate merchants and consumers alike on the technology and to create a consistent experience at the point of sale. Otherwise, adoption will founder.

Morrison agrees: "Human beings are creatures of habit. I think they're willing to try something new, whether they do it out of initiative or out of force," he says. But "if it's not a consistent experience, they will go back to what they know is consistent"—dipping or swiping a credit card. Regardless of the networks' marketing pushes, Morrison doesn't expect adoption rates to move until the majority of POS locations offer a uniform and seamless contactless experience.

Habit likely will play a role in which method of contactless payment consumers ultimately use, too. Ryan says consumer choice is paramount, and merchants should be prepared to accept contactless payments via all three—cards, mobile wallets, and wearables.

Kobos and Donnelly, however, foresee contactless cards paving the way. "That's likely because cards are the more familiar, future-proofed form factor for consumers, while mobile payments still face technological limitations like device battery life," says Kobos.

Using a card is "a lot less complicated than figuring out how to use an Apple Pay," says Donnelly.

That's moot, of course, without more contactless cards in consumers' hands. One possibility that could help financial institutions deal with the expense of issuances on the heels of EMV—and increase relevancy of mobile wallets—is instant digital card issuance. The ability to "apply for the card, but then also provision it into a mobile wallet … so that [consumers are] able to start using it wherever they want right away" has been a topic of conversation with FIs, processors, and other payments players, says Morrison.

Regardless of which form factor comes out on top, contactless is another step on the road to a growing omnichannel environment that's often talked about but not frequently executed, says Donnelly. "I think it's more than just saying, 'Okay, we can speed up the transaction, we can make it a little easier for customers to pay,'" he says. It's moving the industry toward a consumer-focused payment experience. ***TT***

Josephine Rossi is editor of Transaction Trends. *Reach her at jrossi@contentcommunicators.com.*

Make plans now to attend the Contactless Task Force Initiatives panel discussion on October 4 at the ETA Strategic Leadership Forum in Dana Point, California. For more information on the session and the rest of the agenda, visit www.electran.org/events/slf18.

ismagilov/iStock/Getty Images

Partnering With Software Vendors

A guide to help ISOs and acquirers strategically build their ISV/VAR partnerships

By ETA Payment Sales and Strategy Committee

As consumer demand for seamless retail experiences grows, so too does the need for integrated software solutions to meet that consumer demand.

Software as a Service (SaaS) is a $70 billion market. Partnering with an ISV can be an efficient way for merchant service providers to round out their customers' software needs and address gaps in their existing suite of products, without taking on the burden of developing new software in-house. Many software vendors offer white-label products that can be scaled up and integrated quickly. Including software in your merchant offerings can increase customer retention, particularly as merchants come to rely on your software to run their businesses.

The key to successfully partnering with software vendors and developers is to clarify what you're both looking to get out of the collaboration, and establish metrics for evaluating and improving the partnership as it progresses.

Generally speaking, the term "independent software vendor" (ISV) refers to a software producer that is independent of (not owned or controlled by) a hardware manufacturer and whose primary function is creating and distributing software. The difference between an ISV and a value-added reseller (VAR) is that the ISV generally owns the software, whereas the VAR sells it on behalf of a third party.

But the differences don't stop there. ISVs tend to specialize in specific industry verticals, whereas VARs more often focus on specific geographic areas where they can quickly deploy sales agents, according to The Strawhecker Group. VARs often include installation and tech support in their services and focus more on offering software solutions that are installed on the merchant's servers, whereas ISV product offerings tend to be cloud-based. These are very broad distinctions and do not apply to every software vendor on the market, so it is critical to clarify them before formally embarking on the partnership.

Selecting the Right Partner

There are software vendors to suit every merchant vertical and business model. But before you select a vendor to partner with, you must be very clear about your end goal: Are you ultimately trying to get access to the vendor's merchant customers, or are you only interested in its software product? If you are seeking to expand your customer base, there is some due diligence involved. Specifically, you will need to determine how much influence the vendor has over its merchant customers. Will it be able to direct your clients to its services? Is it one of many software

vendors serving its merchants? Does it work with other payment service providers? Asking such questions will help you establish whether the software vendor will be a viable referral channel.

Clear communication is vital here. From the very beginning, you will need to align with your vendor on what access to its merchants will look like. And you need to make certain that personally identifiable information (PII) or other potentially confidential information is mutually protected by all parties.

Of course, if you merely want access to the vendor's software offerings, the path ahead is a bit more straightforward. However, partnering with a technology provider can create friction if you have your own software that needs to integrate with the vendor's software. It is important to test-run these integrations before deploying them to your merchant customers. Additionally, even if you have already tested transactions on your software platform, you must test them in the software vendor's environment as well—particularly after any integrations take place. Some software vendors may require additional integrations with Salesforce, Oracle, or other enterprise solutions. Others may require the use of multiple gateways.

Certification may introduce additional layers of friction. While onboarding a traditional vendor can be a time-consuming process, certifying a software vendor is even more complicated, as the scope of testing and certification is considerably increased. The more "moving parts" the vendor has, the more complexity they will introduce into your own processes. This is not an insurmountable obstacle, and, in fact, complexity can expand your capabilities and merchant offerings. But it is vital to prepare for it well in advance and coach both parties—your sales team and the vendor's team—on navigating the integration, testing, and certification process.

Beyond the technological component, logistical elements require clarification before you finalize the partnership. For example, what is the status of your vendor's employees—will they be contractors, or will they be employees of your company? Will you share revenue? Soft incentives can be very effective, but you will need to clarify the hard incentive structures (like revenue-sharing and commission) first.

Onboarding Your Software Vendor

Effectively onboarding your vendor will rely on providing it with the tools it will need to successfully sell your product. Even the best software offerings can fail to get market tractions if their strengths are not adequately communicated, or if prospects do not understand that they are an integrated solution. You have the payment sales expertise in this relationship. You can use it to help the software vendor market and promote the new integrated solution. You can coach the vendor in selling on pain points and taking a consultative approach, rather than just selling on cost or fees. Consultative selling can improve retention and protect against unproductive price competition. Consider creating co-branded sales materials or otherwise assisting the vendor with marketing campaigns.

How you onboard your software vendor is critical in setting the tone for your relationship, but the partnership does not stop there. If you do not actively manage the relationship on an ongoing basis, you risk losing the vendor to a competitor due to neglect. One way to manage the partnership is to jointly set and evaluate goals. This should be done on an annual basis, and ideally more frequently than that, and it should include open discussions about pricing. The vendor may have a different approach to evaluation than your organization; the key is to find metrics that reflect both parties' satisfaction with and confidence in the partnership.

Partnering with a software vendor can tremendously expand merchant service providers' capabilities. Such partnerships can allow service providers to keep up with their merchant customers' demand and flexibly adapt to new developments in the market. After all, investing in technology is how our industry stays nimble and innovative. ***TT***

ETA's Payment Sales and Strategy Committee is responsible for identifying, developing, and promoting effective business practices pertaining to the distribution and sale of electronic payments–related products and services.

ADVERTISERS INDEX

Adriana Bello

As head of cross-border trade at PayPal, Adriana Bello led development of the company's fourth annual global cross-border commerce report, which surveyed more than 34,000 consumers from 31 countries about their shopping habits.

Here, Bello responds to *Transaction Trends* about the study, the potential impact of tariffs on consumers' appetite for international shopping, and what it means for U.S. merchants that rely on international online sales.

Overall, how much of an impact could a trade war have on U.S. merchants selling internationally?

Even if U.S. merchants must pass along the costs of tariffs to their shoppers, international consumers will likely still look to them when they shop online. The key reason is that many are purchasing from U.S. sites not because of price, but for other reasons. For example, the majority (54 percent) of Chinese shoppers come to U.S. e-commerce sites for "higher product quality." Similarly, the majority (56 percent) of Canadian shoppers look for "access to items not available" in their country when purchasing from the U.S. …

… Overall, cross-border shoppers will still look to U.S. merchants—in fact, one fifth (21 percent) of international shoppers surveyed rank the U.S. as their top destination for cross-border online shopping, making it the second most popular market.

We've heard a lot about China, but your data indicates merchants selling to customers in Mexico or parts of the E.U. could be harder hit—why?

Shoppers from Mexico and some EU countries cite price as their top consideration (59 percent in Mexico, 52 percent in France, and 49 percent in Italy) when making purchases from U.S. websites. Since these consumers are more price sensitive compared to other regions impacted by tariffs, their shopping behaviors are more likely to change if tariffs increase the price of buying goods from the U.S.

Which merchant segments are/could be affected?

With tariffs on steel and aluminum already in place, everyday items like home appliances, or grocery products like beer or soup cans, may already be feeling the impact. Our report found that consumers who shop online internationally are most likely to purchase clothing/apparel (68 percent) and consumer electronics (53 percent). Should additional proposed tariffs kick in, these two categories could feel the repercussions.

If China devalues its currency to retaliate, could we see U.S. merchants losing out to Chinese competitors?

The rising trade war escalations could mean merchants in both countries lose should consumers become increasingly weary of making purchases. However, Chinese shoppers are largely motivated to purchase from the U.S. for factors other than price—higher product quality, access to items not available in their country, and trust in product authenticity.

What can payments professionals do to help their merchant clients as this plays out?

Have the right insights about [their] international customer base so [they] can effectively tailor and target [their] marketing dollars. For example, social media marketing is worth the investment in China, as 45 percent of Chinese consumers who shop cross-border say they typically navigate to international websites to make a purchase after seeing a call-to-action on social media. Further, offering a secure, convenient payment method is a must, as "security" and "convenience" of cross-border trade payment methods [are] top consumer [priorities] across countries.

Tariff conversation aside, what types of goods are most popular for cross-border purchases?

Clothing, footwear, and accessories make up the most popular cross-border purchase category, with 68 percent of online shoppers surveyed saying they've made an international purchase from this category. Tied for second are consumer electronics and toys, which 53 percent of online shoppers surveyed have purchased cross-border. Buyers are likely purchasing cross-border for these items because of better prices and/or because the items are not available in their home country, which are the two main drivers of cross-border shopping globally.

Which regions are emerging markets for global shoppers?

After China and the U.S., Western European markets, such as the U.K. and Germany, are the most popular cross-border destinations for global shoppers, followed by Japan.

Any other trends or global behaviors worth noting?

Yes. Mobile and tablet online purchasing is growing and approaching nearly half of all purchase volume in some of the world's most populated countries. According to our report, in China, 53 percent of purchases are made on a mobile or tablet, 48 percent in India, and 45 percent in the U.S. With the exception of Eastern Europe, purchases on mobile and tablet devices make up 30 percent or more of total payment volume across the world.

Attitudes [toward] cross-border shopping also vary across regions, with North Americans one of the most likely to be loyal to global or home websites. Saving money, free shipping, and a secure way to pay continue to drive international purchases among cross-border shoppers surveyed, while shipping costs and concerns around speed and quality of delivery are the most cited deterrents for global shoppers. ***TT***

—Josephine Rossi

Smart Retail Solutions

A920 Intelligence of a full Point-of-Sale solution in a Handheld device
E500 All in one Android Tablet and Integrated Payment Device
Sleek designs that make them look more like a tablet than a payment terminal.

PAXSTORE

PAX's modern and secure Advance Management Platform for partners and developers to utilize with the PAX Smart Retail Solutions.
www.paxstore.us

PAX

US Headquarters:
8880 Freedom Crossing Trail, Jacksonville, FL 32256
+1-877-859-0099 | sales@pax.us | www.pax.us

Paysafe:

Take your business to the next level. Plug into Paysafe.

Plug into the New Big in payments. Plug into Paysafe.

- Expand your reach with a leading, global payments provider
- Create a program that works for you and your goals
- Increase your earnings with a broadened suite of products and value-added services
- Receive the support you need to help you manage and grow your business
- Capitalize on technology to support efficiency and growth
- Work with a transparent partner you can trust

Plug into Paysafe:

Twitter @PlugIntoPaysafe | **iso.sales@paysafe.com** | **www.paysafe.com**