Summer 2019

TRANSACTION trends

THE OFFICIAL PUBLICATION OF THE
ELECTRONIC TRANSACTIONS ASSOCIATION

SCRATCHING THE SURFACE

A deep dive into the online exploitation of stolen card data

ALSO INSIDE:

Vital®: The seriously smart point of sale.

Vital is a better choice.
For you, and your merchants.

- Perfect for merchants of all sizes
- Extremely competitive and consistent pricing
- Reliable, friendly, and superior support

Bring your customers more with Vital.

Click here to learn more.

TSYS®

Vital®

contents

The Official Publication of the Electronic Transactions Association Vol. 24 | No. 2

features

departments

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

ETA Interim CEO Amy Zirkle
Vice President, Strategic Partnerships Del Baker Robertson
Director, Communications Laura Hubbard
SVP, Government Relations Scott Talbott
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
Michel Coleman, Sam Pfanstiel, 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

Transaction Trends (ISSN 1939-1595) is the official publication, published four 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

Amplifying The Voice of Payments™

One of the essential missions of the Electronic Transactions Association is advocacy. Whether it's before a government agency or a private entity that sets rules and regulations, ETA and its team of advocates work on your behalf to keep policymakers informed and supportive of our innovative and transformational industry. Ask any member of the ETA team to identify the most important tool in their toolkit to accomplish this mission, and the answer will always be the same: you.

Nothing is more effective for ETA's advocacy before public policymakers than the voices, stories, experiences, and expertise of our members as we collectively tell the story of our industry. We connect policymakers at every level of government with leaders, innovators, entrepreneurs, employers, and investors—building bridges that create understanding, respect, and, ultimately, a favorable public policy environment.

There a number of challenges and opportunities in the public policy arena for the payments technology industry, particularly in the state governments. As budgets tighten, federal legislation stalls, and state policymakers look for new ways to raise revenue or make regulatory changes, ETA anticipates that legislative activity in the states will only continue to grow.

ETA is launching a new program called The Voice of Payments™: It Pays To Be Heard, a grassroots project from our government affairs team to give payments professionals working in firms of all industry segments and sizes a central, convenient conduit through which they can get involved directly in ETA's advocacy efforts.

With The Voice of Payments™: It Pays To Be Heard, ETA members will have two new avenues to help them stay informed on and engaged in the top issues and initiatives that are keeping our policy team busy. The first is a monthly The Voice of Payments™ Bulletin, which provides ETA members with a high-level, digestible, and actionable collection of key facts and effects of policy issues happening at the state and federal levels. These monthly bulletins will take the complex machinations of federal and state governments and distill them to the essential information that affects your business—and then provide opportunities for you to directly engage with policymakers to make your voice heard on the issues.

The second new product is an action alert system. These alerts will be sent to ETA members when legislation or other policy developments present the potential to change or otherwise impact their businesses. These action alerts will include tools, talking points, form letters/tweets, and other resources that ETA members can use to easily, conveniently, and effectively engage with policymakers.

ETA also hosts a number of events around the country, including ETA's flagship policy events: the Annual Fly-In on Capitol Hill and the FinTech Policy Forum in Washington, DC. These events continue to grow in scope, impact, and opportunity. ETA provides you—the men and women growing our industry—these opportunities to help you connect directly with members of Congress; regulatory agencies, like the Consumer Federal Protection Bureau and the Federal Trade Commission; and the White House.

ETA's Annual Fly-In will be held on Sept. 11, 2019, and the FinTech Policy Forum is scheduled for Sept. 12, 2019, in Washington, DC. Visit www.electran.org/public-policy to register.

Together, we can work to cultivate a public policy environment that encourages growth and rewards innovation for payments technology companies that are powering global commerce.

Amy Zirkle
Interim CEO
Electronic Transactions Association

Fintech Platform Revenues Surge

Driven by increasing consumer acceptance of fintech-powered solutions, financial technology companies will generate $638 billion by 2024, according to a new study by Juniper Research. The company estimated revenue will reach $263 billion in 2019, a 143 percent growth rate.

In its recently published research, "Fintech Futures: Leading Innovators, Segment Analysis, & Regional Readiness 2019-2024," Juniper forecasted that technologies—such as big data analytics, machine learning, and blockchain—will become the foundation of fintech platforms, changing the way financial services are delivered and driving fintech platforms to become mainstream.

Juniper asserted that, as an increasing number of consumers accept digital platforms for financial services, these technologies will make new use cases the "new norm." The study predicts that developing smart contracts, using artificial intelligence to analyze nontraditional data sources for loan underwriting, and personalizing insurance policies via data generated through the Internet of Things will become common practices.

Chinga_11/Getty Images

Meanwhile, as consumers warm up to fintech, more businesses will attempt to secure future revenue streams by either replicating fintech platforms or partnering with fintech firms that enable them to offer platforms that appeal to new users outside their normal target audience, such as millennials. The challenge, Jupiter reports, will be to integrate these partnerships in a way that minimizes friction and maximizes control of the overall customer experience.

"The distinction between the fintech suppliers and traditional incumbents will blur in the 2020s; digital engagement will become the norm," said research author Michael Larner. "The winners will be those that provide personalization allied to an outstanding customer experience."

Fast Fact

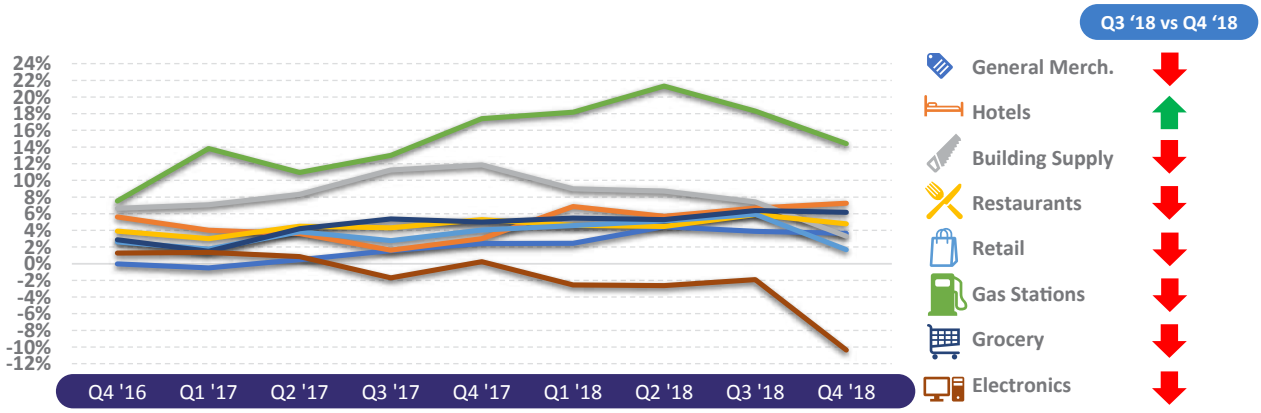
More than half (52 percent) of restaurant and food service industry decision makers foresee **online ordering as having the biggest impact on payments in the industry in the next two years.** That's followed by mobile payments (22 percent), self-order kiosks (14 percent), and cybersecurity (10 percent).

Source: "International Restaurant and Food Service Show Survey Findings," 2019, TD Bank

Infographic

Spending Growth Snapshot at Key Merchant Categories

Year-Over-Year Dollar Volume Growth (Same-Store Sales Growth)



Source: "ETA/TSG U.S. Spending Snapshot," April 2019

Consumers Fear Increases in Identity Fraud With Biometric Authentication

Iaremenko/Getty Images

Although biometric transactions are becoming more commonplace, consumers remain uneasy about the security associated with these types of payments, according to "Lost in Translation: The End of Risk?" The report, released by Paysafe Group in June, reveals the results of research conducted among consumers in the United States, Canada, the United Kingdom, Germany, Austria, and Bulgaria. The researchers sought to study adoption trends and concerns surrounding biometric payments prior to the September 2019 European rollout of Strong Customer Authentication.

Almost half of consumers (48 percent) have authenticated a payment using some form of biometric authentication, according to Paysafe Group, with younger consumers driving adoption. Approximately 69 percent of 18- to 24-year-olds and 61 percent of 25- to 39-year-olds have adopted biometrics in some form. Sixty-one percent of consumers agree that using biometrics is a much quicker and more efficient way of paying for goods or services than traditional online payment methods.

But only 37 percent of consumers believe that biometrics are more secure than other authentication methods, according to Paysafe Group. Thirty-five percent say they do not know enough about biometrics to trust it, and 31 percent are concerned that their fingerprint could be cloned and used to commit fraud.

More than half of consumers (52 percent) are worried that the shift to biometric authentication for online payments will "dramatically increase" identity fraud, and 81 percent favor passwords or PINs for authenticating payments online, according to the research. Two-fifths of consumers do not want companies having access to their personal biometric details.

"Biometrics are a huge opportunity for the payments industry to combat the increasing risk of card-not-present fraud. However, it's not surprising that there is reluctance among consumers to use biometrics as a form of payment authentication when passwords and PINs have been the central pillar of financial data security for at least 20 years," said Daniel Kornitzer, chief business development officer of Paysafe Group. "To overcome this, consumer education is imperative."

Cybersecurity Risks Persist

A new Trustwave report shows that, despite improvements, the electronic payments industry remains vulnerable to evolving cyberthreats. Detailing the top cybersecurity threats and cybercrime trends from 2018, the "2019 Trustwave Global Security Report" reveals that, although there were fewer data breaches in North America last year, the number of attacks continues to rise globally—and the threats are becoming more sophisticated.

The report indicated a slight reprieve for North American companies: In 2017, the region accounted for 43 percent of data breaches investigated, but that number fell to 30 percent in 2018. Instead, attackers shifted their focus to the Asia-Pacific region, which led with 35 percent of data compromise incidents. Retail continued to be the industry with the highest number of data breaches, accounting for 18 percent (up from 17 percent in 2017), followed by the financial sector at 11 percent. Payment services accounted for 7 percent of breaches.

In another positive development, compromises involving POS systems decreased dramatically—from 20 percent in 2017 to 8 percent in 2018. That downward trend reflects the push toward EMV chip cards. Incidents involving e-commerce infrastructures decreased slightly, from 30 percent in 2017 to 27 percent last year.

Across all regions and industries, the most common type of data targeted was card-not-present (CNP) data (25 percent). Although payment card data comprised 36 percent of incidents, that statistic signifies a steady decrease in CNP events, with the number as high as 57 percent as recently as 2016.The second most common type of data targeted was financial and user credentials, which comprised 22 percent of incidents, up from 16 percent in 2017.

The "2019 Trustwave Global Security Report" is derived from analysis of logged security and compromise events around the world, hundreds of hands-on data breach investigations, and internal research. Although the report shows improvement in areas, such as intrusion to detection, it also reveals increased malware obfuscation, more aggressive social engineering tactics, and more targeted web attacks.

Fast Fact

Last year, 55 million people in the United States used their smartphone to make a payment at a physical point of sale, whether by loading money into a closed-loop mobile app—like the Starbucks app—or by loading a credit or debit card into an open-loop mobile wallet—like Apple Pay, Google Pay, or Samsung Pay—and using it to pay at the point of sale.

Source: "State of Mobile Payments in 2019," ETA Mobile Payments Committee

Kritchanut/Getty Images

Mobile Payment Users Await Contactless Technology

The majority of individuals who embrace mobile payments expressed interest in using contactless cards, according to a new online survey by Auriemma Research. More than 2,000 smartphone users were surveyed about their payment preferences.

Sixty percent of mobile payment users expressed interest in using contactless cards, compared to just over one-quarter of individuals who do not use mobile payments. More than one-third of mobile payment users expect their everyday purchasing experiences—such as self-checkout lanes, grocery stores, vending machines, and public transportation—to improve with contactless payments.

While terminal upgrades to support NFC and EMV contactless technology will make mobile payments an option at an increasing number of locations, that doesn't mean mobile payment adoption will rise. Overall, consumers are uncertain about whether contactless card payments are better or worse than mobile payments, according to the survey: 65 percent say they are about the same, 18 percent say they are better, and 17 percent say they are worse.

"Consumers have been repeatedly asked to change their payment behavior," said Jaclyn Holmes, director of Auriemma Research. "While adjusting to various card payments is easy, the larger switch in the physical mechanism of phone payments takes more time."

Moves & Mergers

Singapore Airlines has partnered with **Adyen**, a payments platform, in a move designed to create a frictionless payments experience for customers when they book online or in-app.

Global Payments Inc. and **Total System Services (TSYS)** will merge in a transaction expected to close in the fourth quarter of 2019, the payments technology companies announced in May. TSYS CEO **Troy Woods** will become chairman of the board of directors, and Global Payments CEO **Jeff Sloan** will serve as chief executive officer of the combined company and also will serve as a board member. The combined company will provide payments technology and software solutions to approximately 3.5 million predominantly small and medium-sized business locations and over 1,300 financial institutions across more than 100 countries, according to a press release.

FortisPay has announced the acquisition of **Zeamster**, a payment gateway. **Kevin Shamoun**, Zeamster CEO, has been added to FortisPay's executive team as chief information and technology officer.

i3 Verticals Inc. has announced the acquisition of Pace Payment Systems Inc., which markets, distributes, and sells payment processing products.

International Bancard, a payment acceptance solutions provider, appointed **John Badovinac** as vice president of integrated payments. Before joining International Bancard, Badovinac ran several integrated payment and partner programs at several large payment processing companies.

Mastercard announced that it has agreed to acquire **Transactis**, a platform that helps businesses deliver bills and receive payment. Mastercard will integrate Transactis technology into its Bill Pay Exchange, which it expects to launch in late 2019.

The board of directors for **Nacha**, a nonprofit electronic payments association, selected **Jane E. Larimer** as the organization's next president and CEO, effective July 1. Larimer, who has been with Nacha for 23 years, previously served as the organization's chief operating officer.

NMI, a unified commerce enablement company, announced that it has appointed three new executives. **TJ Fund** was appointed senior vice president and general counsel and will oversee all legal affairs and mergers and acquisition activity. Fund joins NMI from OpenEdge. **Kate Hampton** was appointed vice president of product and general manager of NMI's operations in the United Kingdom. Hampton previously worked at Global Payments, Accelerated Payment Technologies, and Entrata. **Jennifer Sherman** has been named senior vice president of product. Sherman is a 20-year industry veteran who has previously worked at Oracle, Aptean, NAVEX Global, and Kibo Software. In addition, longtime NMI executive **Nick Starai** has been named NMI's chief strategy officer.

Paya has announced the appointment of **Mark Engels** as chief revenue officer and a member of Paya's executive leadership team. Engels brings 20 years of experience in fintech, most recently as chief revenue officer of PayPal's Hyperwallet global integrated payments platform. During his tenure, he led the company's vertical diversification strategy and expansion into Europe and Asia Pacific. He previously served as executive vice president of business and channel development at SecureNet and held senior leadership roles at various fintech companies.

Paysafe Group has announced the appointment of **Philip McHugh** as its CEO. McHugh replaces **Joel Leonoff,** who is taking on a new position as vice chairman of the company's board of directors. McHugh brings extensive experience of the global banking and payments industries to the role, and an executive leadership career spanning more than 20 years. He joins Paysafe from TSYS, where he was responsible for heading up its merchant solutions division.

Visa Inc. has announced plans to the purchase Rambus Inc.'s payments and ticketing businesses. Rambus payment token technology will enable Visa to extend tokenization capabilities to all types of transactions beyond Visa cards, according to a press release.

Acquirers Expect Highest PCI Compliance Rates on Record

Expectations for PCI compliance are rising among global acquiring organizations, according to a new report released by Sysnet Global Solutions. In its second annual "Acquirer PCI Sentiment Survey," Sysnet surveyed senior executives at 30 global acquirers regarding the state of PCI compliance among small businesses and found that 100 percent of respondents now expect their Level 4 merchant client base to perform at a PCI compliance rate of 70 percent or above.

None of those surveyed indicated 50 percent or less as an acceptable PCI compliance rate, a marked decrease from the 16 percent of acquirers who would have accepted those rates in 2018. Despite this higher expectation, only 11 percent of respondents reported that their organizations currently have a compliance rate of greater than 70 percent.

According to the survey, acquirers also believe that they have more responsibility and a duty of care to their merchants. Eighty percent of respondents want to do more to increase their clients' awareness of compliance matters, a critical task considering that 75 percent of respondents do not believe their merchant customers understand the need for compliance.

The majority of acquirers surveyed (72 percent) also would like to move away from obtaining income through PCI noncompliance fees, and more than half (60 percent) believe that adding merchants to a managed compliance service is a viable alternative to charging for noncompliance.

Gabriel Moynagh, CEO of Sysnet, said that providers that incorporate managed services into their PCI compliance offerings will see higher compliance rates and better security among their merchants. This improves customer relationships and reduces the risks—not only for the merchants but also for the acquirers that are often stuck footing the bill when merchants fold under the hefty fines associated with a breach, he says.

"Current methods of charging fees to force merchants into complying simply do not work," Moynagh said. "We've seen that the key driver for raising compliance rates is that acquirers are now providing a managed service to support merchants through the journey. Not only does this change mean acquirers will migrate from a dependence on noncompliance revenue, but [it] will also provide a preventative and responsible approach, which in turn is driving higher expectations in the industry."

Payments Professionals Convene at TRANSACT

ETA's TRANSACT conference this year featured two refreshed and revitalized events that provided an opportunity to honor members who have contributed greatly to the association and the industry.

On April 30, payments professionals gathered at the Light Nightclub at Mandalay Bay to honor top leaders and innovators in the payments industry at the Visa President's Dinner & Star Awards Gala. A mainstay of the TRANSACT conference, this event was reimagined for 2019, bringing together hundreds of people for a night of collegiality and appreciation for the industry's stalwart leaders. The 2019 Star Awards, which recognize individuals and companies that have made a significant difference in the payments industry through innovation, business practices, or contributions to the association, were presented during a ceremony held after the dinner. Winners were named in the following categories: Business Partner of the Year, Committee Volunteer of the Year, ISO of the Year, FinTech Innovation in Payments, Pay It Forward, and Technology Innovation. In addition, O.B. Rawls IV, president of payment processing North America at Paysafe, was awarded the Distinguished Payments Professional designation.

At the Champagne Recognition Breakfast on May 1, payments professionals gathered to honor two groups of exemplary young leaders in the payments technology industry prior to Apple's keynote presentation. First, the 2019 ETA Forty Under 40 honorees were recognized on the SecureTrust Main Stage. Leaders from Discover Global Network introduced the 2019 class, which comprises individuals whose actions and leadership are driving the industry forward. In addition, awardees of the 2019 ETA Young Payments Professional Scholars Program, which provides support, education, and opportunity to 10 young payments professionals each year, were recognized on the SecureTrust Main Stage. Discover Global Network sponsored both of these programs.

TRANSACT Tech Atlanta

More than 200 payments technology professionals came together in June to network and discuss the dynamic and vitally important small-and-medium business (SMB) marketplace at TRANSACT Tech Atlanta.

The event began with an opening fireside chat with Amy Zirkle, interim CEO of ETA, and Adam Bloomston, CEO of Payscape. Morning and afternoon sessions covered topics including disruption and growth in the SMB marketplace, product delivery and value, partnerships, and leveraging innovation to create practical solutions for SMBs. ***TT***

1. Asif Ramji (left), Worldpay chief marketing and product officer, and Royal Cole (center right), Worldpay EVP and head of North America, accept the 2019 Business Partner of the Year Star Award from ETA Interim CEO Amy Zirkle (center left) and ETA President Kevin Jones (right); 2. ETA Interim CEO Amy Zirkle introduces the Star Awards presentation; 3. O.B. Rawls IV (center left) accepts the 2019 Distinguished Payments Professional Award from ETA Interim CEO Amy Zirkle (left), Henry Helgeson (center right), president of Integrated Solutions at TSYS, and ETA President Kevin Jones (right); 4. the 2019 ETA Forty Under 40 honorees; 5. the Light Nightclub at Mandalay Bay; 6. Visa Presidents Dinner & Star Awards Gala attendees; 7. the ETA 2019 Young Payments Professional Scholars Class.

4

5


6

Save The Date – ETA Events

- **Payments Fly-In on Capitol Hill**
  September 11, 2019, Washington, DC
- **Strategic Leadership Forum**
  September 25-27, 2019, Boca Raton Resort & Club, Boca Raton, Florida
- **TRANSACT Tech San Francisco**
  November 18, 2019, Wells Fargo Connections Center, San Francisco


7

The Ins and Outs of Open Banking

How benefits and challenges will impact expansion of the technology

By Scott Talbott

Thanks to ongoing advances in disruptive technologies, skillful fintech entrepreneurs leveraging those innovations to create new financial products and services for consumers and businesses, and consumers and businesses seeking ways to unlock value and better control their financial lives, open banking has become a reality around the world. The citizens of the European Union countries, the United Kingdom, Japan, Singapore, and Australia, for example, have already borne witness to the benefits that can be derived from open banking.

But what exactly is open banking? It can be defined as a framework in which consumers and businesses are empowered to give third-party financial services providers access to their financial transaction data, within secure online channels. The basic concept of open banking is that the information a bank has about its customers can, with the customer's consent, be made available through a secure channel to a third party. That third party can then take that information, aggregate it or combine it with other data, and offer the consumer an innovative product or service that she or he could not otherwise obtain.

For a clearer understanding of what open banking truly means, it is important to examine the ins and outs of this relatively new offering in the financial services marketplace—and outlining the benefits of open banking to financial consumers and businesses is a great place to start.

Benefits for Consumers

Open banking is consumer-centric. Technologies utilized by fintech companies that underpin an open banking ecosystem empower consumers to better understand and control their financial lives. Open banking offers greater choice and convenience while ensuring customers have control over how their personal financial data is used and shared.

Expanding consumer choice through open banking can lead to numerous benefits, such as enabling price and service comparison shopping, broadening the range of money management and investment products available to consumers, improving credit application processes, establishing new payment initiation options beyond traditional payment methods, and facilitating the creation of new businesses.

For consumers to have competitive markets work efficiently and effectively in their favor, they need access to information about alternative financial products and service providers. With open banking, consumers have the power to make more informed decisions about what best meets their needs.

gadhiya/Getty Images

Benefits for Businesses

In addition to offering increased competition, more attractive prices, and enhanced service levels for businesses to take advantage of, open banking supports business-to-business (B2B) transactions. It facilitates B2B payments between companies, reduces the risk of bouncing checks, automatically reconciles accounts, and offers an easy "know your customer" process.

Building a Vibrant Open Banking Ecosystem

Now that the benefits of open banking to financial consumers and businesses have been identified, it is necessary to explore the core public policy issues that must be addressed for an open banking regime to be trusted and, therefore, flourish.

Consumer confidence is at the core of a successful open banking system. That confidence is directly related to participants' perception of privacy, security, and the protection of their personal financial data. Consumers and business owners alike must be confident in the safety and security of the overall system and trust that their financial data is being used in accordance with their wishes and in their best interests.

Accordingly, an open banking system needs to satisfacto-

rily address issues that have been raised about open banking, including customer consent, protection of personal privacy, mitigating cybersecurity risk, determining the ownership of financial data, and allocating liability among the participants in the event of error.

Let's look at each of these issues and identify how they can be managed effectively to establish a sound, vibrant open banking ecosystem.

Consent. A market-driven set of operating principles and standards can be put in place to address legitimate concerns regarding consent and access to the use of sensitive, personal financial data. Here's how these concerns can be allayed:

- *Opt-In:* An open banking regime generally adopts a strict opt-in approach. Only those consumers and businesses clearly wishing to explore the options made available to them by open banking would participate.
- *Explicit and Informed Consent:* Consent to participate in open banking should be informed and explicit. Relying on implied consent could create confusion and negative backlash. Moreover, customers should be informed of the nature of the personal information being transmitted, the parties to whom it is being disclosed, and the use that is being made of the information.
- *Revocation:* If a consumer opts to provide explicit consent to send financial data to a third party, the consumer would also have the ability to revoke his or her consent.
- *Third-Party Standards:* Third parties having access to, and utilizing, consumers' and businesses' financial information would meet well-understood and mutually-agreed-to market-driven principles and standards before access is permitted.
- *Dispute Management:* Some form of dispute management would be available in the event that consumers or businesses believe that an error has been made.

Privacy. When it comes to the essential requirement to protect the privacy rights of consumers and businesses opting to take advantage of open banking, many jurisdictions already have statutory regimes in place to protect privacy. In these circumstances, the temptation to establish separate and duplicative privacy regimes should be avoided.

Cybersecurity. Always a top-of-mind consideration for any technology-based system, cybersecurity is particularly important when personal financial information is involved. It is doubtful that an open banking system would necessarily increase the risk of cybersecurity attacks. In fact, an argument can be made that open banking can reduce this risk, assuming that a market-driven set of operating principles and standards were in place.

Here's how: The reality is that millions of consumers have already provided their financial information and passwords to third parties outside of a formal open banking ecosystem. Doing so unwittingly increases the risk of cybersecurity breaches through the practice colloquially known as "screen scraping," wherein service providers store unencrypted log-in credentials of customers, increasing vulnerability to cyberattack. An open banking regime can mitigate this risk.

Ownership of Data. Who owns a customer's data? This is a complex question, one that is much debated in policy and legal circles. Many would agree that the customer owns the information about her or his financial transactions, accounts, and investments. Complexity arises, however, when that data is combined with additional information that may be added to the mix by third parties working to create an innovative product for customers. This fine legal question is unsettled and requires further attention.

Liability. Liabilities within an open banking system can arise in several circumstances, including the following:

- Data breaches, be they unintended or the result of a deliberate cyberattack
- Unauthorized payments being made, usually resulting from a data breach
- Defective payments, when a transaction has been wrongly processed—for example, where the amount or the recipient is mistaken.

In addition to establishing sound risk management practices, how do the parties within an open banking system allocate responsibility for addressing liability should any of these unintended consequences arise? The challenge is that nonregulated fintech companies are not required to hold operational risk capital while banks and other regulated financial institutions do face this requirement.

In an open banking system comprised of high-level regulatory principles and market-based governance measures, the best way to allocate risk is for the regulated and the nonregulated entities to enter into contractual arrangements that assign liability amongst them. This could be coupled with a dispute management system for consumers and businesses.

Forging Ahead

Open banking delivers value to consumers and businesses, increases competition in the financial services marketplace, drives innovation, and empowers customers to better control their financial lives. Policymakers and financial industry players worldwide have thought through and confronted head-on some of the challenges that can arise when putting an open banking system in place. Important issues such as consent and privacy can be dealt with effectively and efficiently.

It is clear that the time has come for open banking to be readily available to more financial consumers and businesses in more nations around the world. ***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.

More Mobile

Eleven percent of the U.S. population will be using mobile payments by 2023

By Amy Zirkle

One of the many exciting and significant elements of our industry laid bare on the SecureTrust Main Stage at TRANSACT this year was the extent to which mobile payments are growing and adapting in their value proposition to both merchants and consumers. Any TRANSACT attendee who witnessed the keynote from Apple's Jennifer Bailey, vice president of internet services and head of the Apple Pay team, could tell you there's a lot to look forward to when it comes to the mobile payments innovation we witnessed at the show.

I know what you're probably thinking: This conversation is not new to our ecosystem, and its realization is perpetually just over the horizon. Though in the early stages of adoption, there are measurable—and deeply exciting—trends in the payments marketplace that indicate that mobile payments are quickly becoming a common, convenient, and complementary payments method for consumers.

ETA's Mobile Payments Committee is releasing a white paper this summer that explores the current state of the mobile payments ecosystem, highlighting these very trends. Titled "The State of Mobile Payments in 2019," the report examines in detail contactless transactions at the point of sale that are made with a mobile device, presenting data on adoption, usage, consumer attitudes, and projections for the future. Most importantly, it gives a holistic picture that is actionable and relevant to members working across industry verticals—from merchant-level sales to banking and technology.

For instance, in 2018, 55 million people in the United States used their smartphone to make a payment at a physical point of sale, whether by loading money into a closed-loop mobile app (like the Starbucks app) or by loading a credit or debit card into an open-loop mobile wallet (like Apple Pay, Google Pay, or Samsung Pay). There were 26 million active users of open-loop mobile wallets in 2018, the report finds, representing about 8 percent of the total population and 11 percent of smartphone owners. By 2023, roughly 38 million people in the United States will be using mobile payments, with the user base expanding steadily. The report predicts that 11 percent of the population will be using mobile payments by 2023, less than a decade after the launch of Apple Pay in the United States.

monkeybusinessimages/Getty Images

"The State of Mobile Payments in 2019" also highlights the range of capabilities available in the arena. Examples include dedicated peer-to-peer mobile payment apps like Venmo and Square Cash; payment capability embedded in retailer apps like Starbucks' mobile app; QR code-based apps like Alipay and WeChatPay; and tap-and-pay mobile wallets like Apple Pay, Google Pay, and Samsung Pay. The payments industry is working hard to make paying with a mobile device as natural as swiping or dipping a card, or pulling out a dollar bill.

Factors outside of the payments industry are influencing the adoption of mobile payments; the recent successful introduction of New York City's contactless and mobile payments optimized transit system comes to mind. Similarly, the payments technology industry's own innovations—such as loyalty, integrated payments, and increased contactless acceptance—are driving the scope and utility of paying via smartphone. Combined with wearable devices or digital wallets in connected cars, these elements will result in an ecosystem in which mobile payments are an essential part of everyday life.

The new mobile payments report, then, is essential reading for ETA members as it highlights the complexities and realities of the mobile payments marketplace. And whether the topic is mobile payments or another subject—like international commerce, regulatory changes, integrated payments, payments sales and strategy, retail technology, or something else—ETA's Industry Affairs Department will continue to provide new and comprehensive resources to help our members navigate our changing industry.

Visit *www.electran.org/industry-affairs* to learn more and to download the mobile payments report and other ETA white papers and research available to ETA members. ***TT***

Amy Zirkle is interim CEO of ETA. Reach her at azirkle@electran.org.

Make your business secure

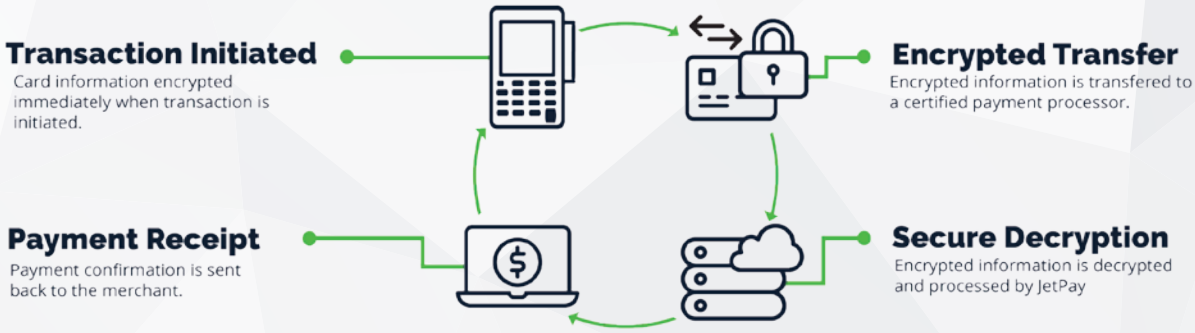
With P2PE and NCR Payment Solutions

Think security

Accepting more types of payments sets you apart from competitors, however, the ability to securely process all transactions is crucial to building good customer relationships.

An extra layer of security

Point-to-point encryption is a security solution that ensure your customer's cardholder data is secure throughout the entire transaction process – even if a breach were to occur. As soon as the transaction begins, all sensitive information is encrypted. This data is then transferred to our secure data center, where it is finally decrypted.



NCR Paymen Solutions works hard to make the complex simple, making everyday transactions into meaningful interactions.

Make your payments more secure.
Visit our website to learn more today!
ncr.com

SCRATCHING THE SURFACE

An in-depth look at how stolen card data is exploited on the dark web and beyond

By Christine Umbrell

Everywhere you turn, there are warnings that your personal information may have been compromised and could be available on the "dark web." Companies offer monitoring services and dark web scans to alert consumers if their Social Security number, personally identifiable information (PII), or credit card data has been part of a breach and has fallen into the hands of cybercriminals.

These threats are concerning—and real. But it's not just the dark web that poses a problem if payment card data is stolen—it's the entire "cybercrime underground," says David Capezza, senior director of payment fraud disruption at Visa. Understanding the sections of the internet where illicit activities are common, and knowing where stolen card data fits into criminal money laundering schemes and other nefarious online uses, is becoming increasingly important for payments professionals as they look to secure transactions and protect merchants and consumers.

The Hidden Layers of the Web

The internet can be broken down into three sections. The "surface web" is the portion of the World Wide Web that is readily available to the general public and is searchable with standard search engines, such as Google and Bing—but the surface web accounts for only 4 to 10 percent of the internet, according to various estimates. The "deep web" comprises the greatest portion of the internet—about 85 or 90 percent—and houses content that is not indexed by standard web search engines; this area is home to private networks, online banking, medical records, subscription information, and services protected by paywalls.

The "dark web," by contrast, is a layer of information that can be accessed through overlay networks. Special software and browsers, such as The Onion Router (TOR), are needed to enter the dark web because much of it is encrypted, and forums are hosted anonymously.

The dark web—about 6 percent of the internet—is home to TOR-encrypted sites and many illegal activities. Cybercriminals buy, sell, and trade corporate data, PII, and other digital assets here, according to IntSights, a security provider. Threat actors sift through massive data dumps looking for credit card numbers, email addresses, login credentials, and more. But fewer than 1 percent of internet users have actually visited the dark web, according to IntSights.

"There is underground trade in stolen personal information, account information, and financial information" on the dark web, says Danny Rogers, co-founder and chief executive officer at Terbium Labs, an information security startup. "Fraud is reaching unprecedented levels."

"We generally think of the dark web as anything that is not openly accessible. It's 'dark' if you can't just walk around and see it—you need special access tools, special permissions, special accounts—things like that grant you or buy you access to it," explains Chris Novak, director of Verizon Threat Research Advisory Center. "Some people refer to the dark web as just what is accessible via TOR. I don't limit it to just that because not all of what we see as dark web is limited to TOR."

The dark web is not indexed, and users need to know exactly where they're going to get to the forums they are seeking, says Luke Wilson, head of intelligence at 4iQ, a digital risk monitoring service. This information is traded and shared on different dark web forums. "You can go to these forums, and … people will ask to purchase certain types of data, or to learn how to do

something," and others will respond with suggestions of .onion sites, where cybercriminals share information. "It's almost like a referral," explains Wilson. "And everything you are doing on the dark web, you are trying to obfuscate who you are."

Cybercrime on the Rise

Concerns over stolen online data migrating to the dark web have grown as more criminals have become "cyberthieves." With the implementation of the EMV standard, card data fraud has shifted from brick-and-mortar stores to online commerce. Since the EMV implementation deadline in 2015, there has been a decrease in in-person counterfeit payment fraud by 80 percent, according to the most recent "Visa Chip Card Update."

"Until a few years ago, criminals managed to get a lot of credit card information from POS terminals—anywhere you used your card to swipe it," says Ziv Mador, vice president of security research at Trustwave. Now, "it's a lot more difficult to create skimmers to compromise those cards because they have been encrypted."

From a merchant perspective, "the adoption of EMV worldwide has significantly improved security around brick-and-mortar stores" at the POS terminal, says Capezza. "Small- and medium-sized merchants with existing e-commerce environments are being presented with a newer cybercriminal methodology, which is online skimming—the targeting of online e-commerce environments."

Of all the data breaches analyzed by Trustwave in the company's "2019 Global Security Report," breaches originating from magnetic stripe data comprised 22 percent of compromises in 2017, but only 11 percent in 2018. In contrast, breaches of CNP

Nastco/Getty Images

data rose from 18 percent to 25 percent in that same time period.

One of the most recent and devastating cyberthreats facing merchants is the rise of Magecart hackers, according to Mador. These groups of cybercriminals have been very active in the past two years, stealing credit card data by injecting malicious code into the checkout pages of merchants' e-commerce stores. Magecart groups have been operating since 2015 and are believed to have compromised nearly 50,000 e-commerce sites since then, according to the Trustwave report.

The Value of Stolen Card Data

Payments professionals, merchants, and consumers should understand that as soon as there is a breach of data in any form, "that information is going to the dark web," says John Sedunov, a professor of finance at Villanova University and an expert in alternative investments. "There's a real risk of people's data being accessed on the dark web from data dumps."

Cybercriminals tend to rely on cryptocurrencies for their online transactions—for example, when purchasing stolen card data. As much as 95 percent of dark web transactions are conducted via cryptocurrencies—primarily Bitcoin—which allow criminals to transfer money without revealing their identities, according to Wilson.

Cryptocurrencies are "a fantastic way for [criminals] to launder things, so they can convert *this* kind of currency into *that* kind of currency," explains Novak. "So, if you can get anything into a cryptocurrency, then you can wash it and move it in a variety of ways that makes it very difficult to trace. And if you can then have it come out the other side in the form of a credit card, then that's generally accepted just about anywhere, from a mega-reseller to your mom-and-pop pizzeria. So, in some cases that is an end goal—to try and get it back into a currency that is readily accessible."

Stolen card data is being leveraged in many ways on the dark web, adds Rogers. For example, it is used in money laundering schemes and to turn dark money into "legitimate" funds. The proceeds from sales of card numbers are used for enabling organized crime and gang activities, weapons exchange, trafficking drugs and guns, and many other illegal activities, he says.

Once cybercriminals get hold of card data, they want to monetize it, says Mador. In most cases, "they sell the data to other gangs that know how to use it. There are multiple forums and websites where they can put the information up for sale, and other criminals will buy it and use it. … There are some websites where … every couple of days, there's a new bulk of 10,000 or 20,000 cards put on sale."

Mador says the criminals who purchase stolen cards have different goals in mind. "In one case, they buy merchandise—for example, iPhones, iPads, even gift cards—and sell them. That's basically a money laundering machine because they buy all that merchandise and put it on sale on the open web." This process turns dirty money into legitimate funds that criminals can use to buy cars, houses, and more.

In addition, gift cards have become a popular way for criminals to turn stolen card data into money. Mador points to websites where people can advertise gift cards and sell them for a

PCI Compliance: An Important Starting Point

aurielaki/Getty Images

The first step in keeping card data from being stolen and sold on the dark web is compliance with standards put forth by the PCI Security Standards Council (SSC). "We are the preventive area—we are trying to prevent that information from ever getting onto the dark web," says Troy Leach, chief technology officer for the PCI SSC. For preventive measures, "most important is to have a plan for how you process payments," says Leach: For example, do you know how you process payments, and can you trace where payment data might be found? Can you limit the number of devices or people with access to data? "The more you limit, you can focus your security attention to a more limited, manageable group of devices," suggests Leach.

It's also necessary to diligently check in on the security controls, says Leach, to make sure they're operating as expected. Be aware that new risks are always popping up.

Leach also notes the importance of considering who is responsible for data security at each company. In some breach instances, new staff members in security positions simply may not have been educated on PCI and the requirements in place to help protect payment data. "It's not just the technology training, but also the people [who have] the responsibilities of security and PCI compliance," says Leach. "There's a lack of training for people coming into new roles."

Currently at PCI SSC, recent standards have focused on introducing more robust controls to be proactive in the design to include security. PCI SSC also recommends that companies ensure that the integrity of good security remains intact, and ensure that the services and software are dynamic in preventing attacks, according to Leach.

"Educate those directly involved in the installation. Good software and hardware can be undone by poor implementation," he says.

discounted price. "Many people sell gift cards for a legitimate purpose," he explains. "However, [cybercriminals] put up gift cards for sale as a mechanism for money laundering. We see sites on the dark web, and even on the open web, offering gift cards that were purchased using stolen credit cards for many different chains—retail stores, fashion stores, restaurants, and so on."

Those who purchase stolen credit card information on the dark web benefit from increasingly sophisticated offerings, tailored to their needs. "[Hackers] used to sell cards in a 'dump' that includes 50 or 100 credit cards, and you would have to figure out which one" was still active, says Wilson. "Now, they sell individual cards for X amount of dollars, and you can go and very quickly [make fraudulent purchases] before the card is deactivated."

"There are sites out there where they 'rack and stack' them, and say how much exactly a specific card is worth," agrees Wilson. "For example, 'Here's a Mastercard, and it's from somebody in the Denver area, and it has this amount of credit limit.' So, an individual will pay X amount of dollars in cryptocurrency to have access to it." They may be purchasing a card number on the dark web for $50 that has a credit limit of $10,000, explains Wilson.

Some criminals organize stolen card data by ZIP code, according to Novak, "because it makes it harder to [conduct] fraud detection," he says. This is because criminals can purchase cards to use in their own geographical locations to limit the chances that their transactions will be flagged.

Some fraudsters offer a form of "money-back" guarantee to individuals who purchase stolen cards. "Many of them offer an alternate card for the next six hours if the one they purchased doesn't work," says Mador. "It's a kind of insurance that you will get the details of another stolen card instead, if the card you purchased is invalid."

It's also important for consumers and payments professionals to understand that one stolen card could end up on multiple dark web forums. "You can have a breach on the surface web—then 15 to 20 different [sites] on the dark web might be selling that data," says Wilson. "From one breach, all these different groups are going to do something different—maybe combining data from one breach with another breach or maybe selling the data to conduct business email compromises," or other criminal endeavors.

A Growing Problem

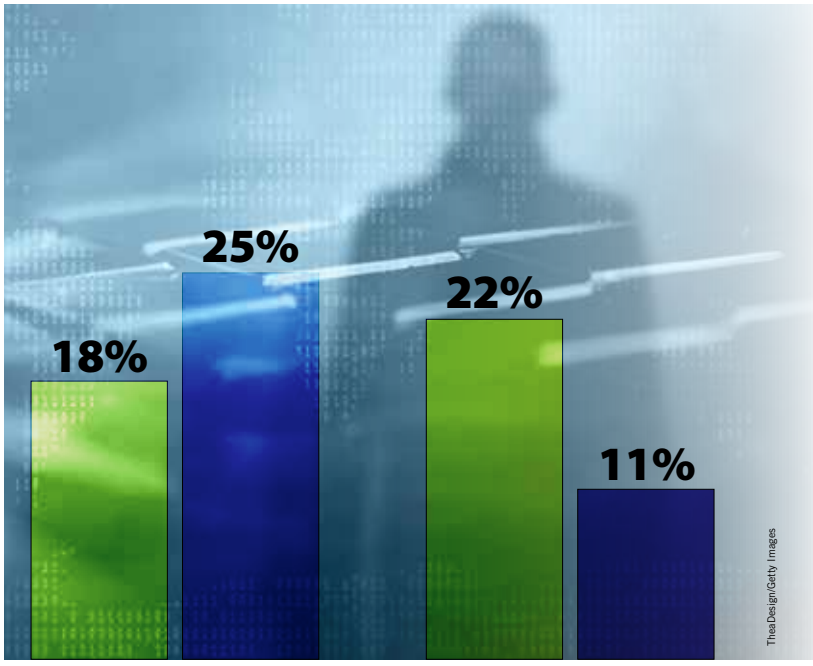
Once stolen card data hits the dark web, it can be hard to track down just where it lands, and it can be even harder to prosecute offenders.

"Many of these forums are owned by people who live outside of the U.S., where American law enforcement cannot put their hands on them," says Mador, citing Europe, Russia, Latin America, Asia, and Israel as areas where forums have been hosted.

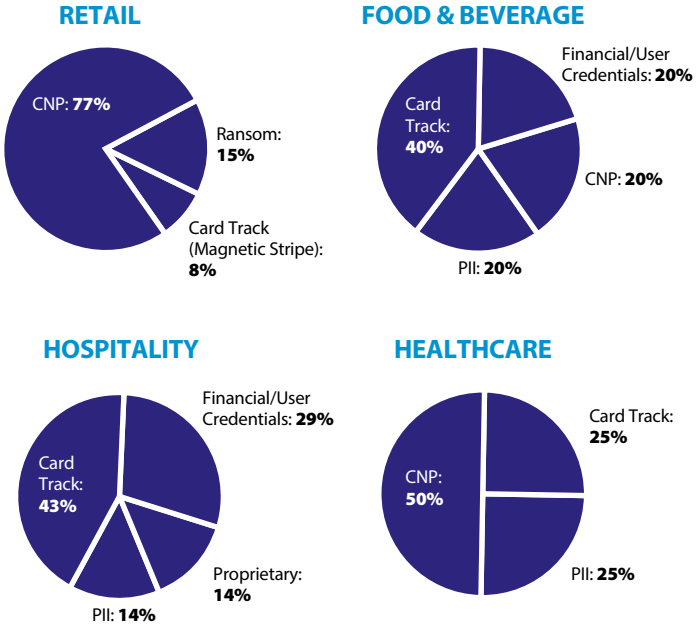
In addition, criminals on the dark web follow a "code of conduct" designed to protect their illicit business interests. According to Mador, cybercriminals in many underground forums adhere to strict rules that are regulated and overseen by "administrators," just to "make sure that people don't scam each other." For example, "when people are accepted to those forums, they start off with a very low 'reputation score,'" explains Mador. "As they conduct business and never scam each other, their reputation rises." These forums are "created and run for the purpose of conducting business between cybercriminals in a fairly trusted environment—as much as they can have."

WHERE DOES STOLEN CARD DATA ON THE DARK WEB ORIGINATE?

The "2019 Trustwave Global Security Report" documents a rise in card-not-present (CNP) data being exploited and a decrease in card track data being exploited since the EMV migration.



MOTIVATION OR TYPES OF DATA TARGETED, BY INDUSTRY



Source: "2019 Trustwave Global Security Report"

Forum administrators also impose "sanctions" on individuals who break their rules, Mador adds. "Their reputation score will be damaged, or they will be identified by the administration as a scammer. In the worst case, they might dox them, and reveal the identities of these individuals—their email addresses, Twitter handles—just to run that person out of business," he says.

"Often the forum administrators on the dark web share information, so once a person is doxed or has lost his reputation in one forum, that is going to affect him on other forums," Mador adds.

How Payments Professionals Can Help

Given the growing cybercrime underground, payments professionals should be aware of the dark web and illicit activities all over the internet, and aid merchants and customers in securing payment card data before it is breached. "Be aware of the data that you have and try at all costs to protect it, but also understand what the typical threats might be that are targeting you," says Wilson. "You have to be on the proactive side of understanding what those threats are."

"BY THE TIME THE DATA IS IN THE UNDERGROUND, IT'S GONE THROUGH A NUMBER OF STAGES TO GET THERE. SO … **HOW DO WE STOP THE DATA FROM EVER BEING EXPOSED OR COMPROMISED IN THE FIRST PLACE,** BEFORE IT CAN BE ACCESSIBLE BY ANY CRIMINALS?"

—DAVID CAPEZZA, VISA

The first step, of course, is compliance with PCI Data Security Standards, says Novak (see sidebar, "PCI Compliance"). "Then there needs to be education and awareness around what social engineering activities look like because we're finding there's a lot of technical controls that are very effective, if they're done right, at keeping your data secure."

Mador recommends that merchants carry out penetration testing, via a third-party security company, to scan websites and applications on an ongoing basis. "We report when we see security issues—missing patches, nonsupported software, or using out-of-date versions of programs," and then recommend steps for remediation.

"The best breach is the one you never read about," says Capezza. "We work directly with our clients and merchants worldwide to proactively identify potential risks or threats to their cardholder data environments, to their payment systems, or to their networks." Visa has taken a proactive approach with its E-Commerce Threat Disruption Program. "We are identifying malicious command-and-control domains that are owned and operated by criminals to deliver Javascript or skimming malware to the merchant checkout pages," says Capezza. "We are actively seeking the criminal infrastructure out and proactively notifying merchants anytime we identify potential compromises to their merchant environments."

Visa also takes a "prevent and disrupt," approach, explains Capezza, to devalue stolen card data. "By the time the data is in the underground, it's gone through a number of stages to get there. So … how do we stop the data from ever being exposed or compromised in the first place, before it can be accessible by any criminals? … That's' where things like 3DS 2.0 and tokenization really come into play. So that if data is potentially compromised at an e-merchant site, for example, that data has no value if it's compromised," he explains.

Rogers says payments professionals can play a role in disrupting dark web activities by making it less financially profitable. "Be proactive in devaluing stolen card data" quickly, he recommends.

Payments professionals also should become more educated—by relying on industry partners, information sharing consortiums, retail and financial services information sharing and analysis centers—and then educating merchants, says Capezza. And all payments stakeholders can visit Visa's website to see public reports and press releases regarding malware, indicators of compromise, mitigation, and protection.

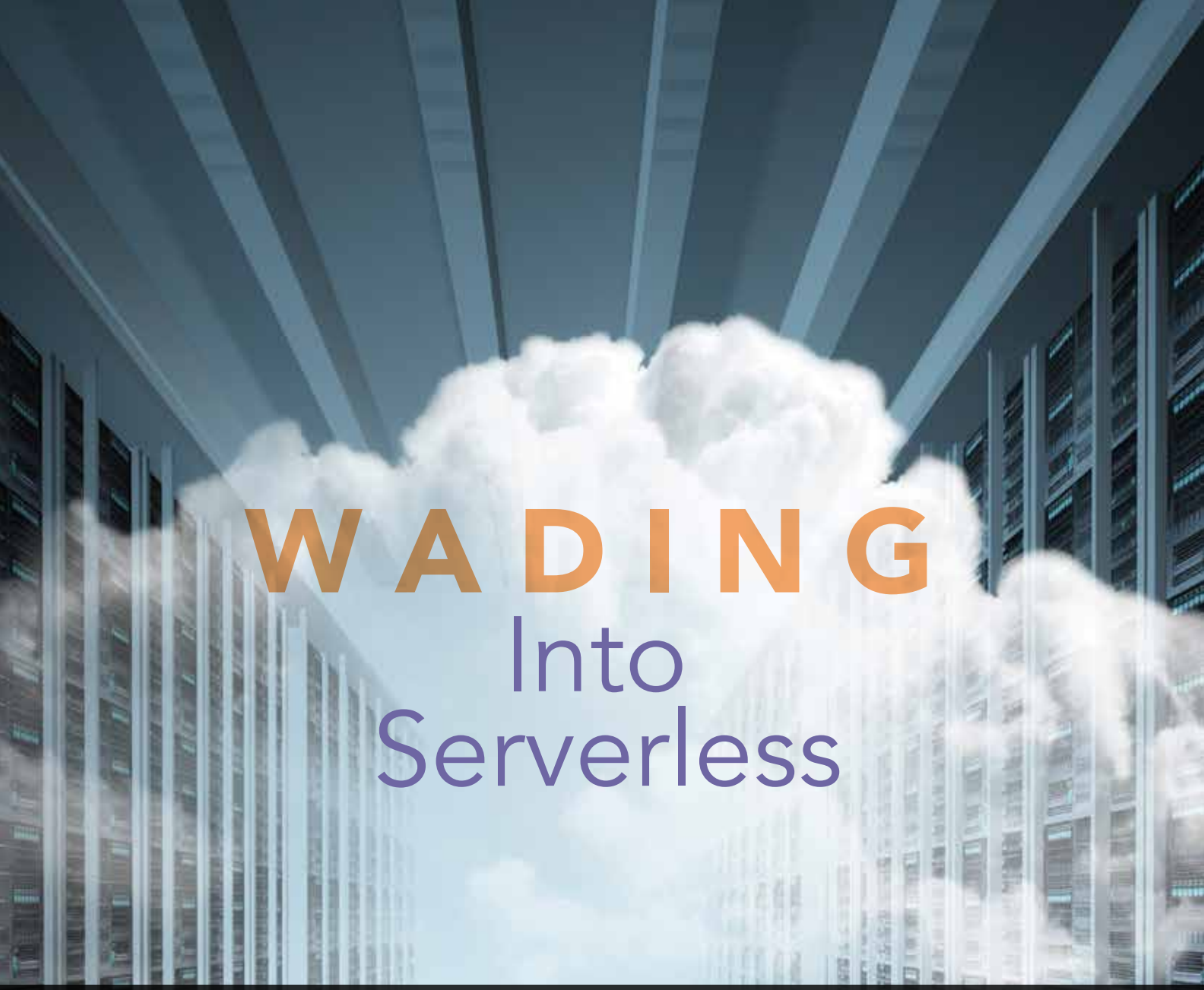
A Look Ahead

Capezza predicts the "democratization of the cybercrime underground" in the coming years. After some recent hard-hitting takedowns of cybercriminals by U.S. and international law enforcement, there's been a shift away from some of the larger marketplaces that were only accessible in the dark web. "You have seen criminals move more toward the deep web and surface web. And you also see criminals working more peer-to-peer—via direct communication channels, moving away from the centralized marketplaces," Capezza says. The landscape where these criminals are operating "is undergoing a shift and a change, and that's something to be aware of."

Unfortunately, Novak believes that growth of criminal activity on the dark web will continue. "With things like cryptocurrency, ransomware, cryptojacking—all of these things that allow these criminal groups to bring in more money" enable illicit activities. "This is not a problem that's going away, and even if you secure something in one place, it could pop up somewhere else. You need to do your due diligence all the time."

"It's an evolution—there's always a changing landscape," adds Wilson. "You can protect against one thing today, but [cybercriminals] will change their tactics, techniques, and procedures. You want to be in that mix of understanding where they're changing and where they're going to next, so you can protect your company and your clients." ***TT***

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



WADING Into Serverless

Payments professionals who have tested the cloud-computing waters explain the benefits and challenges of serverless computing

By Michael Coleman

These days, pretty much anyone with a smartphone or an internet connection is familiar with using remote servers to store and manage computer data, a practice called cloud computing. But the cloud isn't just for saving family photos or sharing work documents anymore. Increasingly, businesses, including payment processors, are turning to a cutting-edge cloud function—serverless computing—to handle a litany of tasks traditionally handled by in-house computer architecture.

In a nutshell, serverless computing is a cloud-computing model in which a cloud provider, such as Amazon, Google, or Microsoft, runs the server and relies on code written by client developers to perform specific tasks. Prices are typically based on the amount of resources consumed by an application,

buchachon/Getty Images

Jirsak/Getty Images

"BEING SERVERLESS ALLOWS US TO FOCUS ON BEING NIMBLE AND DEVELOPING FASTER—RATHER THAN WORRY ABOUT SERVER CAPACITY AND AVAILABILITY."

— KEVIN SHAMOUN, ZEAMSTER

rather than on capacity purchased in advance.

When a predetermined event, such as a payment transaction, activates the code, the serverless platform executes the task. The client doesn't need to tell the serverless provider how many times these events or functions will occur. Typically, serverless clients spend a fraction of a penny each time a function is executed.

Embracing Serverless Technology

Serverless is relatively new to the payments industry, but payment processors are increasingly turning to this new technology for help in managing their data. Some payments industry professionals who have jumped into the serverless end of the information technology pool say that the decision has helped them manage traditional computer workloads and made it easier to comply with the rigorous PCI Data Security Standard.

Kevin Shamoun, chief technology officer for Zeamster, a payments gateway that allows merchants to swipe credit cards and run transactions from any location, says his company has gone almost completely serverless. The company started the transition slowly with Amazon Web Services, a serverless computing provider, six years ago. "Zeamster is an API-first platform that is using serverless to handle all our requests, including transactions and reporting," Shamoun explains. "During peak transaction times, our application scales automatically. Being serverless allows us to focus on being nimble and developing faster—rather than worry about server capacity and availability."

But Zeamster didn't reach this point overnight. "We started slow by design," says Shamoun, who also is vice chair of the ETA Technology Committee. "It's a difficult process to convert your mindset to serverless—it's easier said than done."

While serverless certainly offers an array of attractive IT services, the transition can be difficult for legacy companies that already have extensive in-house computer architecture in place, Shamoun says. Because his company is only eight years old, "we kind grew up with Amazon," he says, explaining that Zeamster added serverless functions as Amazon's offerings became more sophisticated. "We had the luxury of growing up with [Amazon Web Services], and most don't have that luxury." Older payments companies, says Shamoun, "have all kinds of legacy data centers and agreements in place," which make it more complicated for those companies to make the transition.

For startups entering the payment processing realm, on the other hand, Shamoun believes the decision to adopt remote serverless computing instead of buying traditional in-house architecture is easy. "For anybody starting up, I would definitely say it is by far the way to go," he says. "Otherwise, you're going to be stuck in a situation where you have to do some rewriting. You're eventually [going to] want to get to serverless, so why deal with rewriting and migrating software when you can just start that way?"

The Nuts and Bolts of Serverless

The term "serverless computing" is a bit misleading. Serverless still requires servers to process requests and deliver data over a network connection, but the servers are owned by an outside company and operated away from the client's brick-and-mortar business. Server management and capacity planning decisions are completely hidden out of sight, if not always out of mind.

Fayaz Makhani is director of operations for SecureTrust Compliance Services, a division of global cybersecurity giant Trustwave. He says dynamic, nimble, and growing companies are increasingly looking to serverless options to avoid high capital costs.

"This is an emerging area that is rapidly growing," explains Makhani. "The serverless cloud offering is at every major cloud provider now, and many of the smaller providers have put together a service for serverless computing, too. It is something that many of our clients are looking to move

toward because it relieves them of a lot of overhead from the day-to-day operations."

The main advantages to going serverless for businesses, including for merchants and payment processors, are cost and scalability. Businesses can often avoid the whopping price tag for computer architecture, instead contracting out for the exact amount of computing they need.

Serverless computing also permits businesses to ramp up rapidly if they need more computing firepower. This could be a helpful solution for a merchant that anticipates doubling or tripling sales around the holidays but doesn't need all that tech firepower on a daily basis.

Makhani sees the growing move toward serverless computing as akin to contracting for equipment when you need it, rather than buying it. "Imagine today you are an e-commerce merchant and you're doing 100,000 transactions on a daily basis, but we have Mother's Day coming up and you would expect to have 300,000 orders per day," he explains. "Before serverless, you would have to do capacity planning and ensure that you have ample servers and ample time to spin up the servers prior to your workload being generated.

"Today, with serverless, you don't have to worry about that," Makhani continues. "If your transactions go from 100,000 per day to 300,000 per day, the infrastructure is able to scale itself into ensuring your 300,000 orders can be addressed and not have to worry about doing the capacity planning yourself. It allows the merchant to focus on its business … rather than worry about a server stack."

Makhani says the appeal of serverless is primarily that it frees up time and resources spent managing computer technology. In other words, the real value of serverless is not cost efficiency, but time savings. "It's less about eliminating the cost and more about being able to focus on the task at hand," Makhani explains. "Clients are able to focus only on their development and [do] not have to worry about the server stack and the technology stack they would need to support and upkeep to be able to deliver the service."

A general familiarity with cloud computing is helping to win over skeptics at legacy financial companies and major credit cards issuers. "I think because serverless has come in after elastic computing, there is already a bit of familiarity of how cloud providers work, and there is a level of trust that has already been afforded to the cloud providers," Makhani says, "so the transition isn't as much of a paradigm shift today as it was, let's say, five years ago."

Challenges and Opportunities

While there are many potential benefits to adopting serverless computing, making the switch also has its challenges. As business users become increasingly reliant on a specific cloud provider, such as Amazon's AWS Lambda, Microsoft Azure Functions, or Google Cloud Functions, they limit their options for changing course.

"As an organization adopts and matures, it can get tied-in with specific cloud services provided by that specific vendor," explains Adam Salerno, senior director at Colorado-based cybersecurity firm Coalfire. "So, while you can pick up your code and move it easily to a new provider, the equivalent services at a new provider may not be a one-for-one, potentially creating security holes."

Salerno says Coalfire works with plenty of companies in the payments space. "With [payments], in particular, we do see customers using [serverless computing], and it certainly shortens execution time and you're able to gain some performance with it," he says. "But because this is a relatively new technology, there isn't a lot of experience with this type of workload. Organizations and merchants need to consider the new security vulnerabilities this brings up for them."

Peter Wagener, chief technology officer at CardFlight, which provides payment acceptance solutions for small businesses, says his company has embraced serverless computing with good results, although only for a small number of specific functions.

"The uses we have for serverless right now are somewhat limited but very functional," he says. "It very easily handles very spiky loads of requests. We can get 10 requests for a minute versus 1,000 requests in one minute—but the features that are serverless-based work the same way."

Unlike Zeamster, CardFlight doesn't rely on serverless computing for its PCI compliance. "The serverless [providers] actually have only recently come through with compliance-based PCI solutions," Wagener says. "Doing things like handling card data is still relatively new for the serverless environment, so it's not something we've started to use yet.

"But things like handling a device's heartbeat [a periodic signal generated by hardware or software to indicate normal operation or to synchronize other parts of a computer system] and getting certain data off the device ... serverless works extremely well for those types of solutions because it works for any type of load that we may have any given time during the day," he adds.

Salerno and others say serverless offers "an endless amount of things that you can do just based on your workflow and what you want to have happen." And it's not necessarily an all-or-nothing approach to handling a company's IT needs. "It's the perfect playground for dipping your toe in because you can spin things up quickly and test them out, and then shut them down—without having to buy new server equipment to make that happen," he says.

Wagener advises any company considering serverless to do its homework, ask lots of questions, and start small. He also says it's important to understand what you want serverless to do and to write good code to execute those actions. He says a common misconception in the payments industry is that serverless is not secure or able to meet PCI compliance requirements.

"Both of those are incorrect," he says. "You can build fully un-secure and fully un-compliant solutions in traditional or serverless-based solutions. You can also build fully compliant and secure solutions, as well. The biggest confusion I hear is about which problems it's meant to solve." ***TT***

Michael Coleman is a contributing writer to Transaction Trends.

Emerging Payments Security Threats

As cybercriminals employ more sophisticated tools, payments and security professionals embrace new strategies to secure card data

By Sam Pfanstiel

Technology creates new ways for buyers and sellers to interact—whether through newer, more streamlined e-commerce and m-commerce platforms; new in-store points of interaction like mobile checkout or self-checkout; or devices imbued with new payment capabilities, including smartphones, smartwatches, and wristbands. But each new locus of commercial activity also exposes sensitive user data to bad actors. The same innovation that fuels advancements in retail technology also can be harnessed to invent new ways to intercept and compromise financial accounts and data for illicit gain.

Online payment fraud exceeded $22 billion in losses in 2018 and will climb to $48 billion annually over the next five years, according to Juniper Research's "Online Payment Fraud Report: Emerging Threats, Segment Analysis, and Market Forecasts 2018-2023." The FBI's Internet Crime Complaint Center (IC3) received more than 350,000 complaints of cybercrime in 2018, which resulted in $2.7 billion in total losses, according to IC3's "2018 Internet Crime Report."

ETA's Risk, Fraud, and Security Committee monitors the commerce ecosystem for emerging threats and fraud vectors. Below is a sampling of trends observed by committee volunteers who work at leading merchant processors, payment providers, and security companies.

RawpixelGetty Images

Card Skimming

Committee members shared reports of criminals using radiofrequency identification scanners to pick up the information stored on contactless payment cards. However, earlier versions had longer ranges, and in 2013 researchers at the University of Surrey in the United Kingdom were able to receive an NFC contactless transmission at distances of 45 to 80 centimeters (nearly 1.5 to 2.5 feet), according to a study published in the Institution of Engineering & Technology's *Journal of Engineering*. While the range of modern NFC chips is no more than 4 centimeters (less than 2 inches), rendering them more difficult to get close enough to pick up any kind of signal, advances in miniaturization may make skimmers even less detectable.

As early as 2014, the security news site Krebs on Security was compiling reports of ATM skimmers so small they could fit inside the card readers themselves. A criminal could theoretically carry out a man-in-the-middle or relay attack as a cardholder made a transaction using a contactless card at a point of sale.

With contactless cards and EMV technology, it is not clear that skimmers would be able to pick up all of the information needed to successfully counterfeit a payment card—for instance, they may intercept the card number and expiration date, but not the security code. Additionally, if the payment information is encrypted with point-to-point encryption, any information the criminal could intercept would be worthless.

Mouse and Keyboard Jacking

Non-Bluetooth, wireless mice and keyboards (peripheral devices) connect to computers using a radio transceiver, typically a USB "dongle." Attackers can intercept the wireless signals sent between the peripherals and the transceiver from up to 100 meters away and transmit radio signals that mimic those sent by the peripherals. Using these transmissions, an attacker can take control of a computer without needing to physically access it. The vulnerability that affects non-Bluetooth peripheral devices is sometimes referred to as MouseJack.

Bluetooth peripherals are not vulnerable to this type of attack. However, transmissions from Bluetooth devices (dongles, beacons) are typically not secured and may be used to take over a non-Bluetooth mouse or keyboard.

Beacon Jacking

Bluetooth low-energy (BLE) beacons often are used in stores to send location-based, targeted advertising to shoppers' phones. Researchers at George Mason University and Wayne State University, in a study published by the Association for Computing Machinery in 2017, were able to exploit vulnerabilities in BLE beacons, demonstrating that an attacker could, among other things, 1) hijack a BLE beacon to broadcast its own message to nearby devices and 2) track the location of individuals whose devices were picked up by the beacon and associate the emitting devices with specific users.

That said, in most cases hackers were only able to access beacon information because the beacon transmissions were unencrypted or the beacon's location information was static—and thus trackable over time. Encrypting the beacon messages devalues any data that is intercepted, while randomizing the media access control address and other identifying information can mitigate the latter issue.

Terminal Cloning

Criminals who fraudulently obtain point-of-sale devices and link them to merchant accounts are engaging in terminal cloning. This type of attack relies less on technical savvy and more on manipulation, compared to the threat vectors described above.

Terminal cloning attempts tend to target inactive merchant accounts, so the deception goes unnoticed for longer. A criminal might typically access one or more elements of a merchant's credentials—its merchant identification number, terminal ID number, or some other account information, often from transaction receipts. The criminal could then call the acquirer's help desk to authenticate the fraudulent terminal, using the merchant credentials to establish his or her authenticity. A Visa Security Alert from September 2018 reports that some criminals use the terminals to initiate purchase returns to gift cards and then cash out the loaded gift cards at ATMs. The transaction amounts are often in the range of $2,000 to $6,000, according to the security alert.

In response to this type of fraud, some acquirers have established a policy requiring help desk technicians and customer service agents to call back at the merchant's official/listed business phone number to provide an authentication code, rather than providing it when someone calls into the help desk to ask for it.

We can enhance the overall resiliency of our systems so that they can withstand attacks without compromising much or any valuable data.

Preparing for Attack

We cannot anticipate every possible vector of attack on our systems. While some of the cases outlined above have relatively straightforward solutions—often involving modifications to human behavior—in other cases, the failsafe solution may be too costly or cumbersome to implement. But we can enhance the overall resiliency of our systems so that they can withstand attacks without compromising much or any valuable data.

The Payment Card Industry Security Standards Council (PCI SSC) has developed a Software Security Framework to build that kind of resiliency and expand on the principles of its Payment Application Data Security Standard (PA-DSS). Whereas PA-DSS focuses on software development in traditional payment software, with the goal of helping merchants maintain PCI DSS compliance, the Software Security Framework aims to address overall resiliency in software, including bespoke internal software, which the PA-DSS does not cover.

Additionally, we can deploy encryption so that intercepted data are worthless; we can minimize the amount of data we collect in the first place; and we can teach our customers, employees, and end users to spot potential attacks and practice better security habits.

While fraudsters may be getting more sophisticated, so, too, are the payments and security professionals working hard to keep the commercial ecosystem safe. ***TT***

Sam Pfanstiel is director of security solutions—payment solutions, ControlScan, and is vice chair of ETA's Risk, Fraud, and Security Committee.

ADVERTISERS INDEX

James Schneider, PhD

Payments professionals expect mobile payments to gain traction this year, according to James Schneider, PhD, vice president, global investment research, at Goldman Sachs. Schneider was the lead author of the 2019 Goldman Sachs—ETA Merchant Acquirer, ISV, and ISO Survey, which collected insights from approximately 80 merchant acquirers, ISVs, ISO, and payment facilitators (payfacs) to evaluate nascent and impactful payments technology trends.

Here, Schneider shares the biggest takeaways and most surprising findings from this year's survey.

Can you describe some basic trends from this year's report?

From a macro perspective, the most important takeaway is that respondents expect volume growth to remain healthy through 2019, with 76 percent expecting accelerating growth—even after a strong 2018. In addition, pricing pressure appears to be more subdued than it's been in any time over the past five years, with reported average merchant discount rates actually going up across a number of SMB merchant categories this year. Importantly, merchant acquirers, ISVs, and payfacs all appear to be successfully pivoting toward the fastest growing parts of the market, with 55 percent of new sales coming from either e-commerce or mobile channels today—and that's expected to move to 72 percent over the next three years. As has been the case for a number of years, the payments industry continues to see strong new business opportunities in the SMB space, with over 70 percent of respondents expecting to get most of their business from merchants under $1 million in sales.

What was the most surprising finding from this year's data?

One of the biggest opinion shifts expressed by the industry this year relates to the relationship between payments and software. This connection has been recognized by the industry for a number of years with the move toward integrated payments and the emergence of ISVs, but in this year's survey 63 percent of all respondents say they see software as the most effective tool for gaining new business. And 54 percent believe they can get the greatest traction with industry-specific applications, rather than back-office applications, like inventory management and payroll, or marketing/analytics solutions.

In past surveys, a majority of respondents had expressed a preference for partnering with ISVs or other software providers to win new clients. But in this year's survey, almost 60 percent say they prefer to develop applications internally or acquire software assets.

Optimism for future mobile wallet adoption is up among participants, even though actual adoption seems to have plateaued, according to some reports. Why is that?

I think it's fair to say that the adoption rate of mobile payments in the United States has been slower than most people in the payments industry expected at the time of the Apple Pay launch in 2014. At the same time, 92 percent of respondents in this year's survey indicated that they expect mobile payment apps and wallets to succeed—and that's the highest level of positive response we've seen in the past four years. One possible explanation for this apparent disconnect is that our survey doesn't capture expectations around the timeframe for market adoption.

But I do think there have been enough international success stories around mobile wallet adoption—whether it be in the United Kingdom, Australia, or China—that give people confidence that it could work in the United States, too. However, given the sheer size of merchant base, there is still a very large number of retail outlets that need to install NFC-compatible POS devices to ensure that wallets can work ubiquitously for consumers. So while I think there's more confidence that mobile wallets could take off in the U.S., predicting the timing of adoption is clearly more difficult.

What does the data have to say about the future of ISOs compared to ISVs and payfacs, and how does that compare to previous years?

We have been tracking the shifts between ISVs and ISOs in our survey for several years now, and the trend is consistent: ISV residuals continue to increase, while ISO residuals are moving lower—and, in fact, this has accelerated in this year's survey. ISVs are also finding new industry verticals to penetrate with software applications. And while full-service restaurants, education, and nonprofits are the biggest sources of new sales leads today, in three years the focus is expected to shift to hospitals, financial/legal, and the government sector.

In terms of payfac models, the industry is clearly split between those who believe that the model will succeed or struggle over the long run. Factors cited for success include the ability of payfacs to invest more heavily in technology and drive faster client on-boarding—while the biggest risks are viewed as potential financial liability and lack of operational know-how.

Based on the data and your own observations, what's your take on the future of contactless cards?

Like mobile wallets, contactless cards are likely to be a technology that sees slow adoption until critical mass is achieved in the installed base. As I mentioned earlier, it could still take time before the vast majority of merchants have NFC-enabled terminals that are enabled to accept contactless cards. And while the U.S. has lagged far behind the rest of the world in terms of banks issuing contactless cards, there are signs that this is changing. Before 2019, less than 2 percent of cards issued in the U.S. were contactless. But based on public announcements by [some large] U.S. credit card issuers, there could be over 100 million contactless cards issued by the end of this year. ***TT***

Plug into
Paysafe:

Your success is our success.

Want a payments partners that provides more than exaggerated promotions and sub-par support?

At Paysafe, we're not about false promises. Instead, we're in business to exceed your expectations, and help build and grow your business.

Partner with Paysafe and receive:

- Hyper-competitive residuals and bonus programs to maximize earning potential.
- Access to a wide array of products and value-added services to increase earning potential.
- Dedicated support and all of the sales and marketing resources you need to be successful.
- Opportunities to tap into different business segments and expand your portfolio.

Stop settling for sub-par support.

Plug into Paysafe today and learn about all of the ways we can help transform your business. Visit:

www.paysafe.com/partner-today

Smart Retail Solutions

PAX
Your Payment Partner of Choice

The most innovative payment solutions that are elevating the checkout experience.

Taking Payments to the Next Level

ARIES8 | E500 | E700 | A920 | E600

A diverse lineup of solutions with multiple functionalities, suited for any merchant's needs.

PAXSTORE

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

877-859-0099 sales@pax.us www.pax.us

PAX
Your Payment Partner of Choice