Exclusive: Read, Learn, and Earn ETA CE Credits PAGE 12

July/August 2017

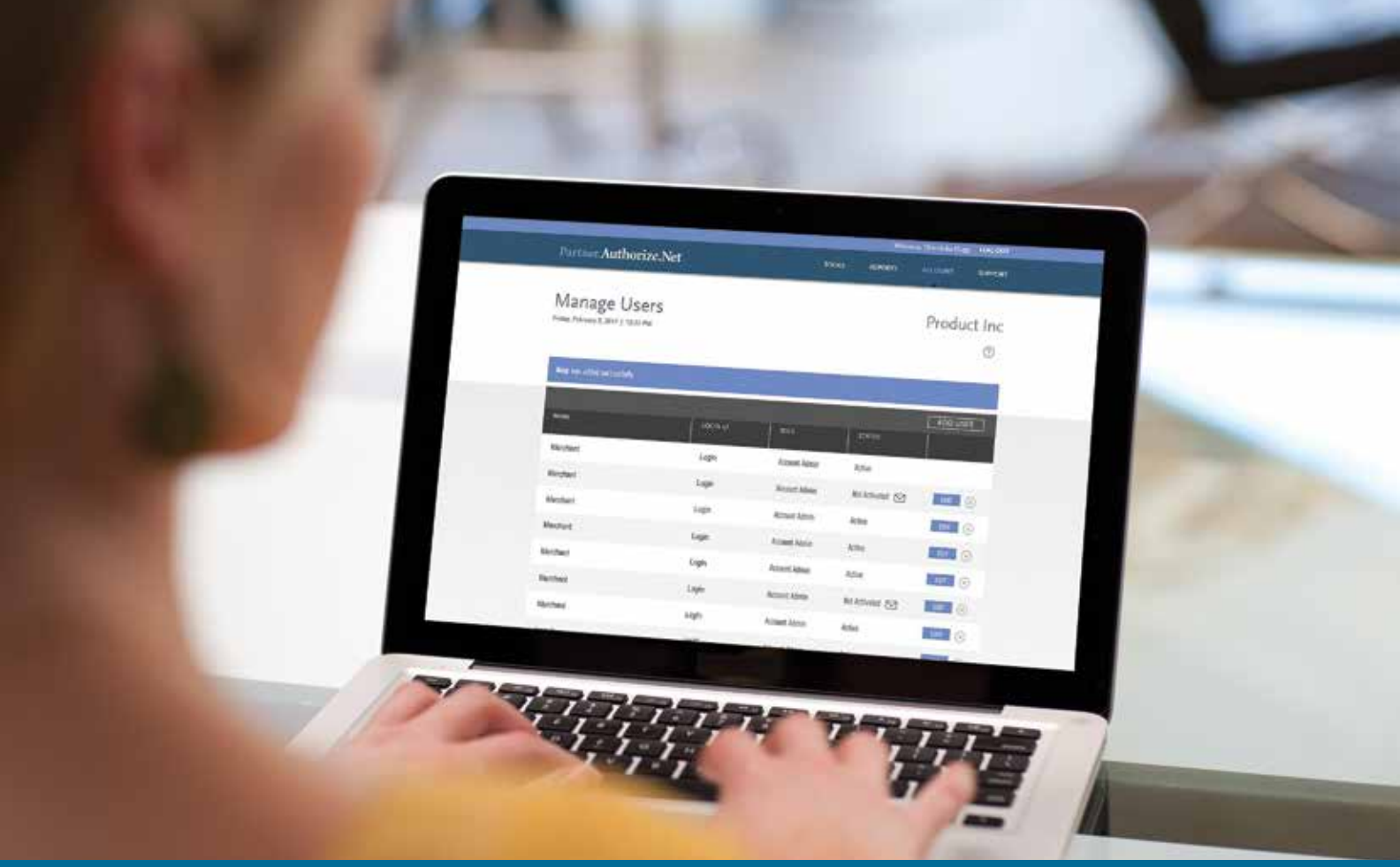
TRANSACTION trends

THE OFFICIAL PUBLICATION OF THE
ELECTRONIC TRANSACTIONS ASSOCIATION

IoT Rising

Defining, securing, and profiting from the Internet of Things

ALSO INSIDE:



Improved Ways to Manage your Portfolio

If you like saving time, you're going to like our new Partner Interface.

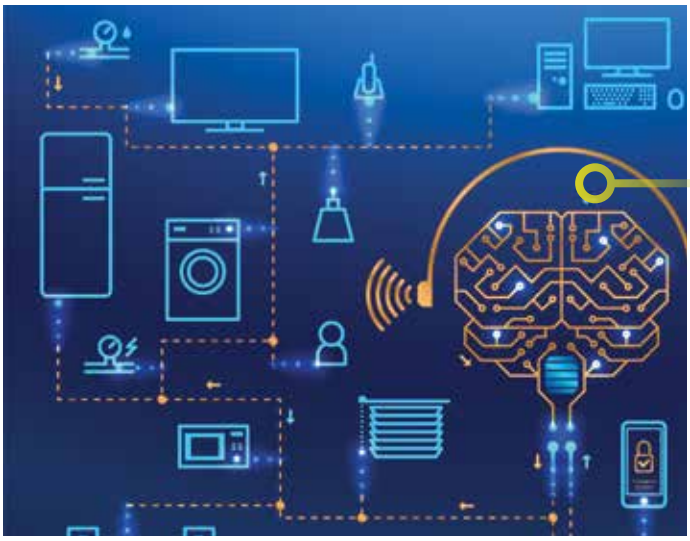
- Improved user administration
- New pricing management
- Simpler merchant boarding

Check it out at **https://partner.authorize.net**

Authorize.Net®

contents

The Official Publication of the Electronic Transactions Association Vol. 22 | No. 4



features

departments

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

ETA CEO Jason Oxman
COO Pamela Furneaux
Vice President, Strategic Partnerships Del Baker Robertson
Director, Communications Meghan Cieslak
SVP, Government Relations Scott Talbott
Vice President, Industry Affairs Amy Zirkle
Director, Regulatory Affairs Philip (PJ) Hoffman
Director, Education & Professional Development Jessica Mosley

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

Subscriptions: 202/677.7411

Editor
Josephine Rossi

Editorial/Production Associate
Christine Umbrell

Art Director Janelle Welch

Contributing Writers
Mike D'Emilio, Brandes Elitch, Josephine Rossi, Scott Talbott, and Christine Umbrell

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

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

ETA SLF: Payments On-Point!

Standing at the helm of the companies changing commerce is an invigorating place to be, but keeping up with the dizzying rate of change within the industry can be a challenge. Fortunately, ETA has you covered! Each year, at the ETA Strategic Leadership Forum (ETA SLF), payments' top executives connect, recharge, and chart the future of our fast-paced industry.

This October 3-5, don't miss your opportunity to join our industry's top echelon of decision makers and power players in Dana Point, California, for a payments event like no other. ETA SLF gets straight to the point on payments—because it is an executive gathering, our keynote speakers and each of our panelists are curated to deliver the impactful, forward-thinking insights that illuminate the issues that matter to you today. At SLF, you will enjoy concierge-driven networking events and ETA-facilitated introductions across the entire payments industry. Connect with C-suite leaders from companies revolutionizing commerce like Alipay, Apple, First Data, Google, Mastercard, and Paypal—just to name a few.

ETA SLF is a unique experience because it is the only event where you have the chance to expand your circle beyond the company bubble to include new partners that can forward your business in a beautiful and luxurious resort setting. At ETA SLF, you finalize game-changing deals while you hit the green, you pitch your start-up to an investor while networking on the Laguna Cliffs, and you sit next to your future collaborators while enjoying fine dining. This meeting feels like an indulgent escape, but it consistently delivers the best return on investment of any payments event!

This year is sure to be a game-changer, as ETA has some big news to reveal! Don't miss your chance to have a front-row seat as history is made when we roll out a major new initiative.

Elevate your company through engaging with your peers at ETA SLF. Registration is open now and is limited. Take advantage of superior networking and the chance to get to work and learn with payments' top leaders. I'm looking forward to seeing you at ETA SLF!

Jason Oxman
Chief Executive Officer
Electronic Transactions Association

A SUPERIOR *POINT* OF CONTACT

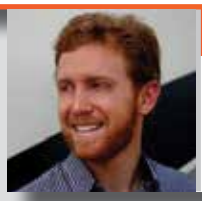
ETA STRATEGIC LEADERSHIP FORUM 2017 | DANA POINT, CA | OCT 3-5 | #ETASLF

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

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

ETA STRATEGIC LEADERSHIP FORUM

POWERFUL FIGURES. EXPONENTIAL RESULTS.



STRATEGIC LEADER PROFILE

WOMPLY'S TURNING POINT

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

–Cory Capoccia, President, Womply

Fintech Adoption Expands Internationally

Investment in the fintech sector is gaining in popularity in several countries, according to the results of a new survey commissioned by Blumberg Capital and conducted by Harris Poll. The survey looked at how financial technology is used in different countries, including France, Germany, Israel, the United Kingdom, and the United States. The results indicate that innovations such as mobile wallets, P2P, online cross-border trade, and mobile banking are taking hold in most areas. In addition, the report found new payment technologies—such as Venmo, ApplePay, and PayPal—are gaining ground but have "not yet penetrated all mainstream consumer groups."

Forty-four percent of Israeli survey participants make online purchases outside the country at least once a month, compared to just 9 percent in the United States. Israel also leads the pack in the percentage of adults who use a mobile banking app at least once a month, at 50 percent. Adults in the other countries do so less frequently: United States (38 percent), United Kingdom (37 percent), France (35 percent), and Germany (28 percent), according to the survey.

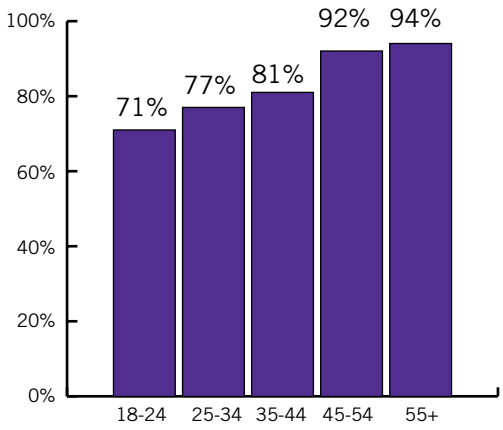
Despite fintech's progress, some countries remain heavily cash-reliant, such as Germany, where 75 percent of adults still use paper currency and coins to make purchases at least once a week. By contrast, 58 percent of adults in the United States and 47 percent of adults in Israel use cash at the same rate, according to the survey.

Survey participants also shared their concerns regarding fraud during online financial transactions. While those in the United Kingdom (43 percent), United States (39 percent), and Israel (38 percent) worry about scams, hacks, and stolen identities, those in France (31 percent) and Germany (23 percent) are less concerned.

Infographic

U.S. Perceptions of Cybertheft

Older consumers are more likely to agree that the number of criminals trying to steal credit or debit card data is increasing



Source: "Consumer Payment Card Data Security Perceptions," Transaction Network Services, July 2017

Fast Fact

"Fifty-nine percent of card-accepting merchants in the United States **use acquiring or merchant banks for their payment processing services**. Acquiring banks collectively are a clear leader compared to the next most common types of provider—a point-of-sale terminal provider (used by 35 percent of respondents) and PayPal (used by 30 percent)."

Source: "Payment Acceptance in a Complex Environment: Banks, Watch Out," Mercator Advisory Group

U.S. POS Systems Remain Vulnerable

When it comes to cybersecurity, breaches involving POS systems were more common in North America than in other countries, according to the "2017 Trustwave Global Security Report." The report compiles intelligence and statistics from Trustwave researchers regarding breaches that occurred across 21 countries in 2016.

"Merchants' slow adoption of EMV chip card readers in the United States again resulted in POS attacks accounting for the largest share of occurrences in North America," according to the report. "Researchers expect those attacks to diminish as more merchants adopt the technology and consumers grow more familiar with it. In the meantime, North American shoppers should always choose the chip when possible."

In their global analysis of breaches, the researchers also noted the following:

- Almost half (49 percent) of incidents occurred in North America.
- Twenty-two percent of incidents affected the retail industry.
- Sixty-three percent of breaches targeted payment card data (33 percent targeting magnetic stripe data and 30 percent targeting card-not-present data).

Cards Overtake Cash in Australian Economy

For the first time, Australian consumers conducted more transactions via credit and debit cards than with cash, according to the "Consumer Payments Survey" published by the Reserve Bank of Australia (RBA). More than half—52 percent—of all transactions in Australia were made with cards, while 37 percent of transactions were made with cash during the 2016 time period.

"The data show that Australian consumers continued to switch from paper-based ways of making payments such as cash and checks, toward digital payment methods—particularly debit and credit cards," according to the survey findings. "Cards were the most frequently used means of payment in the 2016 survey."

The survey also found that younger Australians are choosing debit cards over credit cards, while those over 30 generally have a mix of debit and credit cards. "The difference between age cohorts appears to be because younger consumers are increasingly using debit cards for payments that they would previously have made in cash, whereas other age groups have substituted cash with both debit and credit cards," according to the RBA report.

Cash continues to be used more frequently than cards for transactions of less than $10 in Australia, according to the survey.

U.S. Consumers Increasingly Shift to E-Commerce

New technologies such as connected home devices, virtual reality, streaming television services, voice ordering, and drones have made digital shopping easier and more integrated into everyday life, and more than three quarters of shoppers believe the online customer experience will eventually surpass the brick-and-mortar customer experience, according to a new report from Walker Sands. "Future of Retail: The Connected Consumer and the Changing Face of Commerce" analyzes the retail practices of more than 1,600 U.S. consumers and delves into how developments and technology in e-commerce have altered the retail and the consumer shopping experiences.

The study found that the numbers of online shoppers are growing:

- Nearly half (48 percent) of consumers prefer to shop online rather than in-store.
- Twenty-nine percent of consumers shop online at least weekly, rising to 37 percent of millennial shoppers.
- Nearly two thirds (65 percent) of consumers have mobile shopping apps on their phones.
- Eighteen percent of consumers have made a voice purchase through Amazon Echo or another digital home assistant.
- More than one quarter (27 percent) of consumers own some kind of in-home smart device, such as a smart appliance (16 percent), thermostat (14 percent), or smart lights (13 percent).
- Twenty-four percent of consumers own a voice-controlled device such as Amazon Echo (16 percent) or Google Home (6 percent), while an additional 20 percent plan to purchase one in the next year.

While these trends demonstrate more Americans are leveraging online and mobile payment options, the report also finds that some consumers—including millennials—still seek "the deeper brand experiences they have traditionally been able to get in store." Among the 18- to 25-year-old consumer group, 58 percent prefer to shop in a physical store, compared to 46 percent of 26- to 45-year-olds.

"The majority of consumers (61 percent) now shop online at least once a month. But more than half of shoppers still visit physical stores at least weekly, demonstrating the ongoing importance of the brick-and-mortar experience," according to the report.

Moves & Mergers

BIllingTree has expanded its leadership team, and has appointed **Bryan Schreiber** as CFO. Schreiber will oversee the company's expansion plans to spearhead growth and drive revenue in new and existing markets. In addition, **Kathy Baker, ETA CPP,** has been appointed director of risk and underwriting, and **Steve Recchia** has been hired as director of sales.

Global Payments Inc. has announced an agreement to acquire the communities and sports divisions of ACTIVE Network from Vista Equity Partners.

Ingenico, an omnichannel payments company, has acquired Bambora, a collection of companies that enable the acceptance of a variety of payment types online.

Mastercard has announced it has entered into an agreement to acquire Brighterion Inc., a software company specializing in artificial intelligence.

North American Bancard Holdings has closed on its acquisition of T**otal Merchant Services**.

Paysafe Group has announced it expects to acquire all of the assets of Delta Card Services, the holding company for **Merchants' Choice Payment Solutions**.

Stripe has acquired Payable. The acquisition was reportedly designed to make it easier for platforms and marketplaces on Stripe Connect to meet their tax reporting obligations.

PayPal has completed its acquisition of TIO Networks Corp., a cloud-based multichannel bill payment processing and receivables management provider.

B2B/B2P cross-border payments platform **Transpay** has expanded its leadership team, appointing **Peter Shore** to general manager and **Kevin Gallagher** to senior vice president, global sales.

British payments processing firm **Worldpay Group** has agreed to be acquired by **Vantiv,** a U.S. merchant acquirer and payments processing firm. The newly formed combined group will bring together executive leadership from both companies. Vantiv CEO **Charles Drucker** will serve as executive chairman and co-CEO with Worldpay CEO **Philip Jansen** serving as co-CEO of the combined group as well. **Stephanie Ferris**, current CEO of Vantiv, will serve as CFO to the combined group.

Add 'Policy Expert' to Your Résumé

How in-person meetings with members of Congress shape the future of payments

By Scott Talbott

At the base of it, despite the seemingly complex and nuanced nature of our political system, establishing contact and expressing your views to your elected officials at the federal, state, and even local levels is the most fundamental element of a democracy and advocacy. Representatives are called representatives for a reason; their job, above all else, is to represent you, their constituent, in the halls of government. Communicating your expert industry views to your representatives is paramount to establishing good public policy—and good public policy can increase your ability to serve your customers. One of the most effective ways to get your message across is a face-to-face visit with a member of Congress.

Payments issues are in the spotlight with policymakers in Washington, DC, and it's vital for the payments industry to make our voice heard. Congressional offices must deal with a myriad of complex issues, so your voice is needed to provide clear advice about how to think about the modern payment world. Through smart, strategic—and articulated—grassroots advocacy and in-person, traditional contact, you can help direct the attention and interest of key influencers. Although results may not be immediately evident, personal advocacy efforts can often be effective.

As your association in Washington, we're always here to help facilitate meetings with policymakers. Your legislators want to hear from you, their constituents, about the important issues facing the district, the state, and the country. It is your expertise and real-world experiences that make your voice and input valuable in shaping public policy. According to survey results from Congressional Management Foundation's "Perceptions of Citizen Advocacy on Capitol Hill" report, 95 percent of the representatives surveyed rated "staying in touch with constituents" as the most critical aspect of being effective legislators.

In fact, our annual fly-in is coming up on September 13. This event is designed to provide you with the opportunity to meet and build relationships with your elected federal legislators and staff. We'll meet with members of Congress who serve on the two Congressional Payments Caucuses and federal regulators to discuss issues facing our industry and to provide insight into how our industry works. Participants will receive a briefing package with their

individual schedule, maps, talking points, and other materials to assist with their respective meetings. Your entire ETA government affairs team—Rebecca Cantrell, PJ Hoffman, and Grant Carlson—will lead groups of ETA members in discussions of the latest in payments technology, data security, and other current topics.

The next day, ETA is hosting its annual FinTech Policy Forum where industry leaders, members of Congress, and regulators will discuss the intersection of technology and public policy on such topics as privacy, data protection, Internet of Things (IoT), mobile technology, online small business lending, the continuing convergence of traditional and new players, and helping the underserved. Please plan to attend both events and earn your stripes in DC.

Whether it is during these two or any other ETA policy events, your participation is powerful. Our payments industry is critical to the American economy, and we will all have a role to play in advancing it. You are the voice of payments. Raise your voice and make it heard!

I urge you to take a minute now to learn about ETA's advocacy efforts by visiting www.electran.org/public-policy. Please explore the website and familiarize yourself with the public policy issues that can affect your company. Make it a priority to stay abreast of legislative developments and contact your elected officials. ***TT***

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

SOLVING for IoT Security

What are the risks and responsibilities for payments?

By Josephine Rossi

It's been called a game-changer and the next Industrial Revolution. It's been heralded as possibly the most important technological innovation in history. It's also a little hard to define. We're talking, of course, about the Internet of Things (IoT).

Ask professionals from around the payments community for a definition of an IoT-based payment, and you'll likely get varied responses. For some, it is the natural evolution of e-commerce; for others, it's a distinct concept centered on how a purchase is initiated—by machine rather than man. Still others weigh whether the device fits the description of a traditional computer, which can get tricky considering that mobile electronics, such as tablets, essentially behave like computers.

Direct connection to the internet also seems to be a point of contention. For example, a purchase made with a smartwatch containing payment credentials over an NFC interface may or may not be considered an IoT-based payment, depending on whom you ask.

Even outside of the payments world, the definition of IoT in general remains fuzzy. The global professional engineering organization IEEE developed an 86-page "all-inclusive definition," and the latest version resides on the organization's IoT Initiative web portal as a "living document." Visitors are invited to contribute to the "ever-changing definition of IoT" via the comments section.

Given the disparity in defining IoT, conversations about securing payments via IoT are equally diverse. Sources point to multiple risks and solutions, many of which are similar, or even identical, to those that the industry has discussed for years. They also offer up opinions about stakeholder education and the profession's responsibility to be accountable for future products introduced in the market.

Inherent Risks

The October 2016 distributed denial of service (DDoS) attack on Dyn, a company that controls most of the internet's domain name system infrastructure, arguably gave the general public its first glimpse into the breadth and depth of connected devices—and hackers' ability to infiltrate on a broad scale. According to Dyn, a "significant volume of attack traffic originated from Mirai-based botnets," which infected IoT devices around the world and ultimately led some of the most popular websites on the internet to go dark. Since then, security experts have detected "much other malware" targeting IoT devices, according to IT security and training firm Infosec Resources, which predicts the number of IoT botnets to grow in both number and maleficence.

The Dyn attack did not specifically target the payments system, and a May analysis from Aite Group says attempts to penetrate existing card-not-present platforms "will likely be no more (or less) successful than current hacks on payments." However, with more than 28 billion devices expected to be connected by 2021, it is feasible to assume payments' vulnerability could increase as IoT scales, the payments ecosystem evolves, and new use cases emerge.

"The most significant risk from IoT, greater than the traditional risk of e- or m-commerce, is that the IoT is connecting billions of sensors, each with its own address," says Thad Peterson, senior analyst with Aite Group and author of

'Obvious Market Failure' Leads to IoT Security Bill

At press time, four senators introduced bipartisan legislation—Internet of Things (IoT) Cybersecurity Improvement Act of 2017—to improve the cybersecurity of internet-connected devices used by the U.S. government.

"Under the terms of the bill, vendors who supply the U.S. government with IoT devices would have to ensure that their devices are patchable, do not include hard-coded passwords that can't be changed, and are free of known security vulnerabilities, among other basic requirements," according to a press statement from the office of Sen. Mark Warner (D-Virginia), one of the bill's co-sponsors. The bill was drafted with input from experts at the Atlantic Council and Harvard University, and companion legislation in the House is expected soon, according to a Reuters report.

"While I'm tremendously excited about the innovation and productivity that Internet-of-Things devices will unleash, I have long been concerned that too many internet-connected devices are being sold without appropriate safeguards and protections in place," Warner said in the press statement. "This legislation would establish thorough, yet flexible, guidelines for federal government procurements of connected devices. My hope is that this legislation will remedy the obvious market failure that has occurred and encourage device manufacturers to compete on the security of their products."

In addition to the vendor requirements, the IoT Cybersecurity Improvement Act of 2017 also would:

- direct the Office of Management and Budget to develop alternative network-level security requirements for devices with limited data processing and software functionality
- direct the Department of Homeland Security's National Protection and Programs Directorate to issue guidelines regarding cybersecurity coordinated vulnerability disclosure policies to be required by contractors providing connected devices to the U.S. government
- exempt cybersecurity researchers engaging in good-faith research from liability under the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act when engaged in research pursuant to adopted coordinated vulnerability disclosure guidelines
- require each executive agency to inventory all internet-connected devices in use by the agency.

"THE MOST SIGNIFICANT RISK FROM IOT, GREATER THAN THE TRADITIONAL RISK OF E- OR M- COMMERCE, IS THAT THE **IOT IS CONNECTING BILLIONS OF SENSORS,** EACH WITH ITS OWN ADDRESS."

—Thad Peterson, Aite Group

the report. "Many of these devices have default passwords installed, and those passwords are easily discovered by hackers," he continues. The report also notes that millions of smaller sensors have no security at all—offering criminals the ability to hack one device to get to another.

The threat of using that connectivity to disrupt payments traffic in a Dyn-style DDoS attack is "significant," says Troy Leach, chief technology officer of the PCI Security Standards Council. "That may lead to the inability to authenticate transactions online if a merchant or processor is being overwhelmed by malicious internet traffic." Making matters worse, most of the exploited devices will reside in the consumer's home and "entirely outside the control or ability for the merchant to secure," he adds. The same can be said of poorly or unprotected wifi connections, which security professionals have long warned could be easy access points for hackers.

Peterson says that most of the overall IoT activity currently is at the enterprise and commercial levels where "there is a greater degree of consciousness about the inherent risks of IoT," but he anticipates that will change as IoT becomes more pervasive in general commerce.

Mindset also concerns Sam Pfanstiel, ETA CPP, certified security professional and solution principal for Coalfire, an independent cybersecurity firm. "I think the biggest thing that separates Internet of Things as being a segment of risk is that these are generally purpose-built devices—devices that serve a particular function, and security is generally not that function," he says. "If I'm building a child's toy, I don't see myself as being in the security business. I see myself being in the toy or entertainment business. Similarly, devices that perform payments as a secondary function—using tokens or third-party services—may think they are free from security responsibilities, but this is not the case."

Instead, device manufacturers are focused on competitive advantage through speed to market or maximizing the user experience. "The last thing on my mind is going to be spending an extra six months on penetration testing, third-party vetting, lab testing. Those are the things that really ensure that I have not introduced a vulnerability into that device," Pfanstiel explains.

Leach agrees that additional risk to payments exists if devices don't incorporate solutions such as tokenization or encryption from the start: "Your refrigerator or washer may want to reorder products and can do so in a secure manner," he says. "But again, if the design does not integrate payment security considerations to minimize risk, then cardholder data could be exposed."

Authentication Problems

Regardless of how they define IoT, sources say that within the scope of payments, authentication is the single most critical security challenge facing the profession.

Tim Sherwin, CEO and co-founder of authentication solutions firm CardinalCommerce, says his firm is focused on ensuring transactions from IoT devices can be properly authenticated to avoid fraud and false positives. He explains that his team has already seen "challenges" stemming from internet-connected personal assistant devices, on-demand cable boxes, and gaming systems.

"Specifically, friendly fraud is an issue—when a child in the home orders something through a cable box that a parent didn't authorize," he says. "Makers of these devices have already put software in place to require a PIN or other code to prevent this. As these devices become more sophisticated and more prevalent, we can expect to see new challenges."

Cardinal, which was acquired by Visa in February, is looking to the newest version of EMVCo's 3-D Secure to address the issue and has built the new specs into its core product.

The 2.0 version of 3DS was developed to "support app-based authentication and integration with digital wallets, as well as traditional browser-based e-commerce transactions," according to the EMVCo website. Sherwin says the new specification "dramatically enhances the amount of data that is used to perform authentication. More data means more informed decision-making by both issuer and merchant, lower rates of fraud and false positives, and fewer challenges."

In an automatic card-on-file scenario, the device, rather than the user, needs to identify itself, explains Philip Andreae, vice president of field marketing for OT-Morpho, a new digital security and identification technology firm resulting from the May merger of Oberthur Technologies and Safran Identity & Security. Shoring up device identity is "an emerging place," he says. OT-Morpho supports the idea of embedding cryptography into device hardware—a secure element that already is used in mobile phones and payment cards. The firm is currently providing embedded secure elements to several luxury connected-car manufacturers, including Maserati and BMW, he says.

"When I boil it down, it's this act of authentication, which we have to secure," Andreae explains. "We have to do it in a convenient and secure way that cannot be spoofed, that cannot be replicated and used nefariously."

When scaling for IoT growth, Andreae, who is secretary of the FIDO Alliance and who also led the team at Europay that developed the standards for EMV, suggests payments professionals look to standards such as WebAuthn, which the World Wide Web Consortium is developing to provide authentication in the internet space. "Then, I'd start looking at biometrics—because sometimes it's not just the object that I want to authenticate; it's the presence of the right individual," he adds.

Education and Accountability

Specific security solutions aside, sources agree that stakeholder knowledge is vital to the future of IoT security.

For its part, the PCI Council is partnering with industry organizations to help innovators and app developers better understand payments security. It is working on "software development practices to educate developers and demonstrate basic security principles are consistently being tested against software within all forms of devices," says Leach.

The Council is concerned with current software practices—namely that most software is updated frequently, is highly customized, and relies heavily on open source. "These are challenges that really didn't exist 10-12 years ago in payments before 'smart' technology" was common, Leach explains.

As a result, the Council is reevaluating its Payments Application Data Security Standard to account for new software lifecycles and agility while also ensuring "integrity and assurance exists for merchants and cardholders that entrust the application to be tested and protect against common threats," says Leach. It will release more information about the new requirements in September.

> "ANYONE WHO TOUCHES THE PAYMENT STREAM **IS NOT ONLY RESPONSIBLE FOR SECURING THAT DATA** BUT ALSO ACCOUNTABLE FOR WHAT HAPPENS TO IT."
>
> —Sam Pfanstiel, ETA CPP, Coalfire

Pfanstiel ponders self-regulation in terms of driving peer accountability. For example, an acquirer could require that devices used on its network adhere to a particular security framework. He also believes strongly in effective third-party risk management—"good vendor agreements, solid vetting, and contractual obligations for security that transcend some kind of arbitrary compliance" and cover appropriate attributes and attack vectors. The "risk of producing another DDoS attack like what happened to Dyn DNS last October—that's huge. That affects the payments ecosystem as well as the entire internet. Just depends on who they want to target next," he explains.

Consequently, education around multiple risk factors, "not just putting your blinders onto payments," would be of value, Pfanstiel says.

Andreae believes strongly in educating stakeholders, too. He sees a void in "simple, easy-to-understand" communication efforts—particularly in the consumer media and among business executives and merchants—that adequately explain security concerns so that stakeholders demand it of their products. Even payments professionals who are not directly involved in the security function, such as those in sales and marketing positions, don't fully appreciate the necessity of effective security measures. "We're educating the people who can provide the answer [to IoT security problems], but we're not educating the people who have to ask the question," he says.

"There's no one really that's not to some degree responsible for the security of the installations that are being placed into the market," Pfanstiel concludes. "Anyone who touches the payment stream is not only responsible for securing that data but also accountable for what happens to it." ***TT***

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

The Future of BITCOIN

The world's first cryptocurrency—and the blockchain technology it introduced—slowly gains acceptance as challenges persist

By Christine Umbrell

Bitcoin—the original cryptocurrency—has made headlines this year, first for a meteoric rise in value over the first six months, followed by a dramatic plunge in July and "split" August 1. Its volatility makes it difficult to predict just what will happen next, and whether more Americans will embrace the concept of virtual currencies. But some of the recent activities in this space provide clues as to the future of Bitcoin and similar currencies.

Bitcoin hit the alternative payments scene in 2009 as the first completely decentralized digital currency, implemented as open source code. The currency was an instant game-changer in that it allowed for transactions to be made without revealing personally identifying information, was operated by a decentralized authority, and offered lower transaction fees than traditional online payment mechanisms. The introduction of the currency also marked the debut of "blockchain technology"—a peer-to-peer distributed ledger of timestamped transactions.

Fast-forward to 2017, and Bitcoin has seen more than its fair share of ups and downs. "There's people from all over different countries doing really amazing, and reckless, things with these types of technologies," says Josh Mather, technology evangelist at Vantiv, who spoke during the "411 on Blockchain" session at TRANSACT. Globally, the currency is most popular in early adopter nations, such as Denmark and the Netherlands, as well as in countries with cash and economic stability issues, such as India and Venezuela. In April, the Japanese legislature

officially categorized Bitcoin as a prepaid payment instrument and passed a law bringing Bitcoin exchanges under that country's anti-money-laundering/know-your-customer rules.

Here in the United States, the currency has seen a great deal of activity in 2017. The price of Bitcoin tripled between January and June, trading at more than $3,000 at its peak. Several events may have contributed to the surge in popularity, including the legislative activity in Japan and the expectation that countries such as South Korea and Malaysia could follow suit. But the value of Bitcoin headed downward in July, falling well below $2,000—and demonstrating the continued volatility of the cryptocurrency.

In a recent turn of events, key miners and developers of Bitcoin have adopted a new way of operating the cryptocurrency, called Segwit2x, in an effort to speed transaction times. But a rival system, called Bitcoin Cash, also has emerged, meaning the Bitcoin market is effectively splitting in two directions.

Unpredictable Yet Intriguing

While the recent fluctuations in value have been concerning to those who leverage the cryptocurrency on a regular basis, "the volatility of Bitcoin over time has decreased," says John Sedunov, professor of finance at Villanova University and an expert in alternative investments. "But it's still more volatile than the price of gold and other currencies. That's a problem for acceptance."

While not a lot of business is being conducted in the United States with Bitcoin right now, many people are using it as a "value store," Mather explains. "There's a lot of people in the U.S., and China, too, that have a lot of money that are storing a lot of value in Bitcoin."

Many Americans are looking at Bitcoin, which is not associated with a central bank, much differently than they view dollars. "I might wake up tomorrow and the value of my Bitcoin may be drastically reduced," Sedunov acknowledges. "The point of having a central bank is, in part, to defend the currency's value."

Linda Coven, CTP, a senior analyst at Aite Group, also sees Bitcoin's ever-changing value as a difficult concept for some potential adopters. "There's a question of how much it's worth," she says. The value of one Bitcoin today "may change tomorrow. That [volatility] is very disruptive in any kind of transaction.... If it's a one-time [transaction], it may be OK. But if you're going to hold on to the [currency], that may be a problem."

In addition to the cryptocurrency's volatility, security issues related to public ledgers moving transactions also give some would-be users pause, according to Tony Rose, director of product, mobile, and emerging payments at Vantiv, who also spoke during the blockchain session at TRANSACT. "With the Bitcoin network, if someone were to hack it and somehow take

Learn more about the evolving role of the blockchain and its implications on payments. Log in and listen to "The 411 on Blockchain" from TRANSACT at www.eventscribe.com/2017/Transact.

Cryptocurrency Options

While Bitcoin was the first, it is not the only cryptocurrency. There are all sorts of iterations available today, with Ethereum and Zcash garnering recent buzz.

Ethereum

Ethereum was developed by Vitalik Buterin in 2013 as a cryptocurrency traded on its own blockchain. Unlike Bitcion, Ethereum can incorporate "smart contracts" into its blockchain; these are computer-based contracts that pay parties once certain conditions have been met and verified.

Ethereum uses many of the same systems as Bitcoin, including blockchains and peer-to-peer networking, to generate a shared world computing platform that "can flexibly but securely run any application users want to code (shared ledgers like Bitcoin included)," wrote Buterin in the article, "What Is Ethereum?" The cryptocurrency "aims to take the promise of decentralization, openness, and security that is at the core of blockchain technology and bring it to almost anything that can be computed."

Massive fluctuations in the price of Ethereum have been similar to those of Bitcoin this year, at times experiencing even greater volatility.

Zcash

Zcash, which launched last October, was developed by the Zerocoin Electric Coin Company (ZECC) as an open and programmable financial system built on the concept of privacy. "Privacy is the only way to ensure fungibility and guarantee that cryptocurrency can be interchangeable as a fluid medium of exchange for users," according to the Zcash website. "Companies need the protection of privacy along their supply chain in order to conduct their business, especially in the context of public blockchains."

Because Zcash is an open-source protocol, ZECC does not control the currency or have special access to private or shielded transactions. Users can send and receive scarce tokens that can be used like cash on the internet. The software that powers Zcash is directly derived from Bitcoin's core software, but it has been modified to enhance user privacy, according to Coin Center. The Zcash network uses modified Bitcoin software to allow users a choice at each transaction: either get paid at a normal address that works transparently just like a Bitcoin or via a private payment address. If two people transact with shielded addresses, the Zcash blockchain will not record the details of that transaction publicly.

Zcash gained greater visibility in May when ZECC announced a partnership with JPMorgan Chase to add ZCash's privacy technology to Quorum, an enterprise blockchain platform JPMorgan built on Ethereum. With the partnership, Quorum can ensure private settlement of digitized assets on a distributed ledger.

Zcash offers "more privacy around where the money is coming from and going," explains Linda Coven, CTP, senior analyst at Aite Group. "It offers the ability to send things without having any idea where they're coming from or going to." Coven notes that the Zcash blockchain is being heavily utilized for sending contracts back and forth, rather than payments: "Using the blockchain and Zcash for trade finance, which is very document-intensive, in a safe, secure way may save money," she says.

over that network, they could control quite a bit of actual value."

Yet despite volatility and security concerns, many Americans are intrigued and are slowly testing the cryptocurrency waters. Sedunov cites three categories of early adopters: people who mine the currency, institutional investors, and consumers. "The anonymity is appealing to some," he says. (See sidebar "How Anonymous Is Bitcoin?")

The market for Bitcoin has been on a slow path to growth since its introduction, says Sedunov, who believes the sluggish pace of acceptance is to be expected of a digital currency. "The technological aspect of it might demand that the time to greater acceptance is longer" than for traditional currencies, he points out. The complicated nature of adopting Bitcoin—which involves downloading software, visiting an online exchange, and remembering a permanent password—comprises a technological barrier that may take some time to overcome.

Addressing Transaction Speeds

There are several reasons why sudden price drops may occur and why some remain hesitant to explore cryptocurrencies. This year, the currency transaction speeds have been slowing—a challenge related to the blockchain technology itself. "A blockchain is a database that has solved some really hard problems in computer science, around the ability to have network integrity, when you have a network of nodes that are trying to have one state of truth," explains Rose.

"Bitcoin is the biggest blockchain out there, currently … it really was solving this data integrity between a distributed network of nodes problem that is the key innovation there. By solving this problem, they've unlocked a lot of really interesting use cases that many people are excited about, with the potential to disrupt the industries—from payments, to supply chain, to health care," says Rose.

But with increasing numbers of individuals making Bitcoin transactions come slower transaction times. "One of the things Bitcoin gets a lot of flak for is that it can only currently process about six transactions per second, so there's really big scale issues with large public networks," notes Rose.

During the first seven months of the year, the average time it took to approve or make an official transaction was steadily increasing, according to Sedunov. Bitcoin transactions are processed in "blocks" that involve complex cryptography. Those blocks are used to record transactions on the Bitcoin network, and, until recently, had a maximum size of 1 megabyte. "When fewer transactions were happening, this was fine—but now there's a backlog," says Sedunov.

Complicating matters, Bitcoin users may choose to pay a fee to have their transaction processed more quickly—meaning that those who pay lower or no fees must wait hours or even days for transactions to be completed. The longer the wait times, the higher the fees for quicker transactions. This is problematic because most Bitcoin users prefer to complete their transactions quickly—before the currency changes value.

Two competing groups have suggested "fixes" to alter the Bitcoin blockchain to solve the transaction delays, and August 1 marked a turning point in the tug of war. "There are two solutions to this problem: Segwit2x and Bitcoin Cash," explains Sedunov. "Both plans revolve around changes to the blockchain, which is the log of all previous Bitcoin transactions. The changes are both related to the size of the blocks in the chain. Bitcoin Cash will expand the size of each block from 1 megabyte to 8 megabytes, while Segwit2x moves some data on to a parallel track and eventually allows the block size to double to 2 megabytes."

Segwit2x seems to be the solution that has the most traction, and key players agreed to adopt the Segwit2x technology around August 1. "However, some believe that Bitcoin Cash is a better solution to the problem," explains Sedunov. "Because there are two different solutions to the problem, separate blockchains will be created, and Bitcoin Cash will be a parallel currency to Bitcoin."

Sedunov predicts that, from a transaction standpoint, Bitcoin Cash should work in the same way as Bitcoin. "However, what will be interesting to observe is whether the prices of Bitcoin and Bitcoin Cash move in parallel," he says. As of press time, Bitcoin Cash was worth only a fraction of the price of one Bitcoin.

"It is uncertain what will happen next, and really it will depend on whether Bitcoin Cash thrives or fizzles," Sedunov says. If Bitcoin Cash survives, the cryptocurrency market will be further fragmented. But either way, if the August 1 changes result in faster transaction times and lower costs, "then this is good news for those who plan to use Bitcoin in a retail setting, and may have the effect of setting a roadmap for solving these problems, should they show up again in the future."

Integrating Into the U.S. Payments Landscape

While Bitcoin is not currently accepted by the majority of U.S. merchants, there are some exceptions. Overstock.com became one of the first retailers to accept Bitcoin in early 2014, and several additional names now accept the currency, including Expedia, eGifter, Subway, Microsoft's Xbox and Windows store, Reddit, Steam, and more.

Some merchants and consumers are trying to get past the stigma first associated with Bitcoin, when rumors swirled about its use for gambling purposes and for other illicit activities. "The reputation holds that the only people who are using it are people who wouldn't want to bank—which most companies don't want to be associated with or be considered 'promoting,'" says Coven. She predicts that cryptocurrencies that are associated in some way with banks—such as ZCash, which is accepted by JPMorgan—may have an easier path to acceptance.

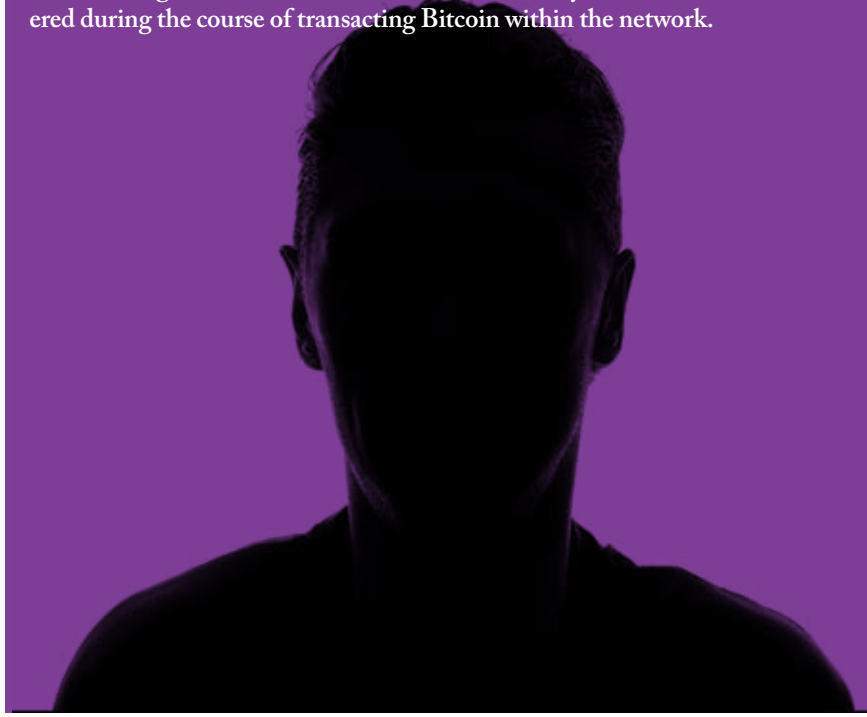
But Sedunov believes Bitcoin's "bad rep" is dissipating over time—and Rose agrees that more legitimate use cases are

How **Anonymous** Is Bitcoin?

Bitcoin is "anonymous but not private," explains the website of Coin Center, a nonprofit focused on cryptocurrencies. "Identities are nowhere recorded in the Bitcoin protocol itself, but every transaction performed with Bitcoin is visible on the distributed electronic public ledger known as the blockchain."

Those who access Bitcoin through an online wallet or exchange service have their personal identities linked to their Bitcoin holdings. "Bitcoin for these users is effectively no more anonymous than a bank account, although this loss of anonymity takes place at the point of entry into the currency and is not a feature of the Bitcoin protocol itself," according to Coin Center.

Users may find alternative entry points to take advantage of the cryptocurrency's intrinsic anonymity by acquiring Bitcoin in a private transaction, as compensation for goods or services, or as a reward for mining. "Subsequent Bitcoin transactions can then be anonymous, since real-world identities are not recorded on the blockchain ledger; the only identifying information recorded there are the Bitcoin addresses, whose corresponding private keys are held by the owners as proof of ownership," according to Coin Center. But remaining anonymous is not guaranteed because a real-world identity could be discovered during the course of transacting Bitcoin within the network.



evolving. "Mexico as a country is about to introduce legislation that accepts [these] currencies as part of their economy," he says. "We have countries, like Venezuela, where they're using Bitcoin because their economy has collapsed."

For more U.S. merchants to begin accepting cryptocurrencies, there will need to be increased consumer demand because retailers will need to adjust their payments infrastructure to accept it, says Sedunov. He also notes that retailers who are considering accepting Bitcoin may feel obligated to accept other cryptocurrencies, adding to the complexity.

Mather and Rose do not believe blockchain technologies and digital currencies are ready to take over the traditional U.S. financial payment system. "But the maturity of a public coin or public token can grow.… . It is possible that given the maturity of these tools, that over time, it could offer at least an alternative or a primary mechanism for a payment system," says Rose.

If and when cryptocurrencies become more commonplace, there may be new opportunities for acquirers. "From an acquirer perspective, our job is to give the merchant money the consumer wants to give them, using technology—whatever technology that could be. If there's ways and new technologies that are emerging that could make the transaction overhead less [costly] to do that, the merchant doesn't necessarily want to set up a bunch of wallets or manage a bunch of public or private keys, so someone still has to do that for them," says Rose. "So there's still a function to provide services around payments. A lot of the different use cases just make the way the current systems work more efficiently, so someone will come and offer those services at a reduced cost.

"Whether it displaces existing legacy middlemen, or those middlemen evolve to offer these services in more efficient ways—that's more the question than 'Will middlemen be removed?' There's always room for services and added value between parties," Rose continues. "A given merchant could go set up a Bitcoin wallet and accept payments from consumers that have gone and done that as well. But there's going to be other players that bring it to scale," he says. "Everyone can benefit from reduced processing overhead and reduced operational processes that can be made more efficient. So I think that's where the real value lies, and that's where the opportunity lies, is to really look at those types of use cases."

Mather agrees that there could be opportunities for growth with the expansion of distributed ledgers. "There is an underpinning shift that will occur in certain areas of the ecosystem, and, depending on how people roll with it, they could become irrelevant, they could become a new player in the market, [or] they could continue operating the way they are, depending on what their role is in the ecosystem," he says.

Mather notes that current technologies would need to evolve before a major transition can occur. "The technology replacement—there's a lot of hard work that needs to be done there, because there's a lot of reasons that a lot of those pieces of technology are in place," he says. "And there's a lot of reasons that these layers of bureaucracy exist, and the regulation exists for these systems. And so when something comes along that offers efficiency and other types of optimizations, people take a hard look at it and start implementing it slowly. No one wants to jump into the system and ruin their mothership. But we may see that transition slowly."

Keeping an Ear to the Ground

The recent surges and dips in value are keeping the experts guessing as to how quickly Bitcoin and Bitcoin Cash will gain greater acceptance. But cryptocurrencies—whether Bitcoin or other iterations—are likely here to stay. "I don't think we can ignore cryptocurrencies such as Bitcoin, but several challenges remain before digital currencies can become viable and commonly used for payments, especially B2B," Coven suggests.

Payments professionals should understand how digital currencies work and determine what types of value they can provide should more merchants accept these types of payments. "This is early-stage technology, so you should try to gain a working knowledge of it. We're trying to figure out what the roadmap really looks like, beyond the hype cycle," says Mather.

While regulations will be needed if cryptocurrencies become more widely used in the United States, regulators are not in a rush to address the issue due to the current limited number of transactions. "The market cap is so small [compared] to other currency exchanges," says Mather. "There probably isn't a push to regulate something like that for currency manipulation, at this point."

Coven predicts we will see the pool of players investing in cryptocurrencies expand as different groups test the waters, and then contract once some are adopted and others abandoned. For the cryptocurrencies to really take hold in the United States, the Fed will have to get involved "and set some of the rules," says Coven. Right now, Bitcoin and other cryptocurrencies are "playing outside the rules" put in place post-9/11 to ensure that banks know their customers, and their customers' customers. "That's what makes this so interesting," she explains. "With Bitcoin, there's no accessible information."

Sedunov doesn't foresee the U.S. government accepting Bitcoin as a legitimate currency anytime soon. In March, the U.S. Securities and Exchange Commission (SEC) denied a request by investors Cameron and Ty Winklevoss to list what would have been the first U.S. exchange-traded fund built to track Bitcoin. The SEC's decision stated that "based on the record before it, the Commission believes that the significant markets for Bitcoin are unregulated. The Commission notes that Bitcoin is still in the relatively early stages of its development and that, over time, regulated Bitcoin-related markets of significance may develop."

Of course, as more digital currencies emerge, increased volume may bring the need for federal oversight to a tipping point. "Then, regulation will probably happen, and that will go a long way toward determining the future of Bitcoin," says Sedunov.

But massive change is not likely to happen overnight. There is plenty of time for payments professionals to develop a cryptocurrency strategy. "Are we going to see payments being replaced? Probably not anytime soon, but certain use cases will disrupt certain areas," notes Mather. "So I would say to an acquirer, try and figure out what the product roadmap really looks like on the horizon." ***TT***

Christine Umbrell is editorial/production associate for Transaction Trends. *Reach her at cumbrell@contentcommunicators.com.*

Acquirers in the Age of IoT

Experts from across the profession contemplate strategies for adapting to the latest innovation

By Mike D'Emilio

With an estimated 30 to 50 billion new smart devices initiating electronic transactions on behalf of their owners by 2020, the effect of the Internet of Things on the payments business will be nothing short of revolutionary, say many experts.

Learn more about IoT and the payments world. Log in and listen to "How IoT Is Revolutionizing Payments" from TRANSACT at www.eventscribe.com/2017/Transact.

"Every time there is a revolution, the stakeholders have to go through an evolution to keep up," says Ruston Miles, ETA CPP, chief strategy and innovation officer at Bluefin Payment Systems. First among these stakeholders are its drivers, the innovators creating new devices. They face a set of unprecedented challenges: higher costs to create smart devices and the software that will animate their electronic brains; complex, emotional barriers to adoption, including the "creepiness" of household goods that watch you like a loyal dog and spend your money like an empowered teenager; as-yet-undefined linkages to payment and order fulfillment systems; and the security risks, costs, and uncertainty that go along with them.

With disruptive new technology comes market turbulence, which is always harder on smaller companies—and ISOs and financial institutions (FIs) are no exception. But a consensus seems to be building that the advent of IoT devices presents more opportunity than danger to smart acquirers. In fact, during a panel discussion on the subject at TRANSACT, Jasma Ghai, vice president of emerging payments innovation at Discover, quoted a projection of "23 percent growth" in overall transaction volume as IoT technology matures.

Miles points to the opportunity this presents to FIs, as they can recommend security solutions, IoT-focused payment gateways, and tech-friendly ISOs. "Many IoT innovators and entrepreneurs are moving fast to market their products, and are likely consumed by a myriad of specifics related to building and marketing the IoT device itself," says Miles. "Payment acceptance is a necessary function for many of these devices."

"What strikes me about the Internet of Things is that most of what needs to exist to support payments in the context of IoT largely exists today," says Ron Carmichael, vice president of global innovation at Elavon. The key is to inform product developers of these solutions and to tailor them to the new requirements of IoT transactions, he says.

Perfecting Partnerships

During the panel talk, experts discussed the path to adoption of IoT devices, and the roles that ISOs and FIs can play in helping to drive it. A good starting point, according to Dan Loomis, director of payments product management at Intuit, is for companies like his to "fall in love with our customer's problem." By recognizing the steep learning curve facing many IoT innovators, service organizations can provide support at the critical early stages that often make or break new ventures. Loomis notes that Intuit, in its current work helping customers ensure that payments are compliant and taxes are accounted for, has already begun providing the tools and services that will prove vital to IoT partners. Easy-to-use software development kits (SDKs) and application program interfaces (APIs), as well as detailed and far-sighted assistance with tax calculation and payment validation, are among the Intuit offerings that Loomis believes will transfer seamlessly to the new requirements of IoT transactions.

Companies have already created mobile-originated transactions that shift the point of sale away from merchant locations, Miles observes. In so doing, they have worked out a

"SCALE IS PROBABLY THE MOST DAUNTING ASPECT OF IOT" FOR PAYMENTS PROFESSIONALS. **"THE VOLUME OF TRANSACTIONS WILL GO UP,** WHILE THE SIZE OF EACH TRANSACTION WILL GO DOWN."

—Ron Carmichael, Elavon

cohesive partnership process thus far. The mobile or handheld blueprint would seem like a logical one for IoT innovators to follow, but, if there is one constant in the hyper-competitive world of disruptive technology, it is to expect the unexpected. Miles worries that the bundling of software and services and more tightly integrated devices and gateways may force some ISOs and acquirers to let go of the payments piece. His advice is simple: "ISOs should be making partnerships with IoT makers now so they are not left behind." Specifically, he sees payment security as a prime opportunity because many innovators are new to the payments industry and need guidance on how to best secure transactions.

Carmichael takes a slightly more optimistic view. He suggests that new players, like Square and Stripe, are not threats but rather drivers of a more proactive mindset. In his view, they force large acquirers to become more aware of merchants lower down on the food chain and inspire them to be more adaptive with their offerings. Guiding IoT developers to solutions such as the contextualization of the transaction— asking questions like, "Does it make sense for my refrigerator to purchase a car?"—will help them save time and money as they build out their security infrastructure. Organizations can offer advice on solutions like data encryption and tokenization, and exchanging devalued data instead of investing in fortresses to protect credit card details and personally identifiable information, say sources. They can begin to sell what Loomis calls "security as a service"—not with massive server-based products, but with the currency of the mind.

Providers of highly usable solutions can help IoT innovators and, by extension, themselves. "The better job we can do of providing well-documented micro-services that are easy to use, easy to integrate, and easy to deploy and maintain," Loomis says, "the faster our industry is going to make inroads in the IoT space."

At Elavon, the focus is on "making integration developer-friendly: supporting lots of different languages for the purpose of being able to initiate payment, allowing developers choice, giving developers the tools they need to be able to easily integrate with our gateways," says Carmichael. He cites examples such as automating testing processes and the certification process for their solutions, providing robust documentation for developers on the integration process, and simplifying registration. "Any advantage we can give the developer in getting to market faster, we think is mutually beneficial," he notes.

Ghai points to the flexibility with which Discover allows companies to use its technology to gain access to multiple wallet providers and tokenization services. "We're positioning ourselves with the right technology and expertise to adapt to the changing payments industry," she says. The website for Discover Digital Exchange (DDX) promises that "retailers and consumers can look forward to the flexibility, ease, and increased security they expect in today's digital world. And as payments continue to move towards digital solutions, DDX is positioned to help support new wallet and token payment options. From smartphones and smartwatches, to fitness trackers and automobiles, to whatever comes next."

Currently 800 million small businesses are using 3.1 cloud-based apps apiece, according to Loomis. By 2020, that number is projected to grow to 8.2 apps per company. The increased demand for these solutions will create inroads for providers to partner with companies as they roll out devices capable of IoT transactions, he says. By assuming a key role in the process, service providers can help underwrite the risk associated with the growing number of devices in these distributed sensor networks. The networks themselves will require a transformation of the underwriting modes and risk models to manage these payments, as well as the devices that those payments are supported by, he adds.

"Scale is probably the most daunting aspect of IoT" for payments professionals, Carmichael says. "The volume of transactions will go up, while the size of each transaction will go down." Capturing this proliferation of small transactions requires "scaling up to be able to support an increase in volume and, at the same time, being more efficient in assessment of each transaction for its appropriateness from a fraud management and a security standpoint... That's where we're making

our investments, trying to be able to grow with the scale of the transacting devices that are out there."

End-User Considerations

As merchants and device companies navigate this new landscape, successful ones will always remain aware of their customers' most urgent needs. The same is true for ISOs and FIs, which would do well to study the full lifecycle of the transaction to identify areas of focus. Ghai says Discover constantly asks, "What pain point are we solving for that partner or consumer?" She says that if there is no clear answer, they go back and begin again. "It is not enough to simply inject payment into a process," she asserts.

Inherent value, such as Discover's Cashback Bonus, must be part of the IoT-based payments equation—as should a consideration of the consumer's priorities, according to Ghai. For example, when a device uses customer behavior to determine that a purchase of some kind is warranted, and then makes that purchase, a simple ping from the card company via text or email informing the customer goes a long way in reinforcing her confidence in the entire transaction chain, she says.

The prospect of IoT devices initiating electronic transactions calls into question the definition of point of sale. "We are seeing a rapid shift toward the customer becoming the point of sale," Miles says. "In this paradigm, a transaction can happen when a customer comes in contact with any payment-enabled IoT device, most of which are owned by the customer, not the merchant. This fundamental change will affect the expectations, solutions, and interfaces for electronic transactions."

With many stakeholders rushing into the IoT space, the race to ubiquity seems like a land grab, sources suggest. Some stakeholders may attempt to build a single, massive platform and consolidate transactions, while others may retreat to niche markets and carefully cultivate value and credibility. While the first strategy might play well with the consumer instinct to "set it and forget it"—to select one payment method and never change it—the latter approach could be better for smaller ISOs and FIs that already serve specific markets. Miles points out that smaller ISOs sometimes have an interesting advantage because they can be more reactive to the specialized needs of IoT providers, while larger ISOs must focus on larger deals.

So much new technology emerging from so many places forces big organizations to look for opportunities to purchase or fund smaller ones with promising talent or strong niche fits. "Like all of the major acquirers," says Carmichael, "we are very closely monitoring what's happening in fintech and particularly in the startup space."

In addition to identifying and adding valuable new offerings, acquirers can improve their IoT readiness by collaborating to define a set of best practices and common standards. Ghai points to initiatives like EMVCo (her company, Discover, is a participant) that can help advance payment technology while avoiding technical fragmentation and instability. Extending a stable technical foundation with secure interoperability to IoT devices will benefit everyone—especially the consumer, she says.

IoT Data Monetization for Manufacturers

Samsung recently announced a new service to monetize the voluminous data shared by IoT devices.

"For the first time, device manufacturers and service providers can tap into an open ecosystem and create service plans that generate revenue directly from the interactions of devices and services," the company announced in a press statement. The new solution offers manufacturers the ability to leverage extensive interoperability features to create new revenue streams and business models, such as hardware as a service.

The goal of the new solution is to help manufacturers recoup expenses associated with offering free and third-party apps and services without passing along anticipated costs to consumers in the retail price of the devices. The ARTIK Cloud Monetization service provides a "complete brokering, metering, and payments system," and it offers manufacturers the ability "to make their devices interoperable with third-party devices and applications, and monetize data usage." The solution "brokers and meters user interactions against the defined plan, and manages upgrades, payments, and revenue share back to the device OEM," according to the statement.

"Samsung is committed to growing the IoT data economy," said James Stansberry, senior vice president and global head of ARTIK at Samsung Electronics. "Samsung ARTIK Cloud Monetization uniquely positions us to help device manufacturers find new ways to make money from IoT and enable more applications for their customers. This is part of our long-term strategy to facilitate the development of secure IoT products and services, promote wide-scale interoperability, and create a platform and business model for an entire IoT ecosystem to thrive. Like the mobile phone industry, IoT will be driven by open systems, interoperability, and support from innovative applications."

There will be a natural tug of war between "frictionless" and "creepy," but the IoT is coming. Older users may balk at advances such as cars that monitor driver behavior and punish immoderation with higher premiums, but younger people worry less about such intrusions into their personal lives. With the right balance, most consumers are inclined to accept products that make their lives more convenient, sources say. "We consistently and continually invest in integrated payments as a key part of our future as an acquirer," says Elavon's Carmichael. "We see more, not fewer, devices being payment authorization points in the future—not just conventional credit card terminals."

An innumerable array of internet-connected devices is already coming online, and very soon will be generating electronic transactions. The fastest and most flexible acquirers will have an advantage in working with them. In this evolving ecosystem, the nimble will survive and thrive. ***TT***

Mike D'Emilio is a contributing writer for Transaction Trends.

Fighting Fraud, Managing Growth

New developments on the horizon following EMV deployment

By Brandes Elitch

EMV has gotten a lot of press during the last year, but the fight against payment card fraud is just beginning. In an October 2016 article, the *Nilson Report* projected that card fraud will grow 42 percent in the next three years, and worldwide fraud losses will approach $31 billion. Problems include the delay of gas station EMV adoption, card skimming, data breaches, systemic problems with the card verification values (CVVs) for online purchases, plus "fallback fraud," where an EMV transaction is processed using the magstripe. That said, the American Bankers Association reports that new credit card accounts are up 8.8 percent year over year, and the total number of open card accounts is now 357 million.

ETA members have been busy coming up with new ways to control fraud and manage the enormous growth in cards. Here are four advances you will be hearing more about later this year.

Mastercard 2-Series BINs. The bank identification number (BIN) is the first six characters of a card number, also called a primary account number (PAN). Card brands have seen increased demand for cards, due to tokenization, mobile wallets, replacement account numbers, and prepaid cards. Each card brand has devised a proprietary solution. Mastercard will supplement the existing range of account numbers (that now begin with a "5"), with a new range that begins with a "2," to effectively double the number of cards it can support. This requires a software update for terminals or changes to a BIN range configuration file or table. Some merchants will require new hardware, if their terminals are too old to handle the software updates. Online payments sometimes use an auto-select feature based on the BIN, which means the customer doesn't have to enter the card brand; thus, they will need an update. Mastercard set a deadline of June 30, 2017, (yes, a few months ago!) for merchants to be able to accept 2-series cards, and it has designed 2-series test cards to test a terminal for compliance. To spur compliance, Mastercard has stated that an acquirer may be subject to monthly fines for noncompliance of up to $25,000, and their small merchant could be fined as much as $100 for accepting a card for a $25 purchase. The new cards will be issued this summer.

Eight-digit BIN. Payment processors have typically designed their compliance strategy around the PCI Data Security Standard, using PAN truncation to render cardholder data unreadable. PCI truncation keeps the first six and the last four digits, and destroys six digits, so an attacker has a one in a 100,000 chance of guessing the original PAN. The proposal for an eight-digit BIN will change these rules. The possibility of an eight-digit BIN and a 16-digit PAN could impact the software on every terminal, merchant website, processor, and card processing network. There are significant issues for back-end systems, analytics, and database and reporting systems, and the cost of changing payment terminals would be meaningful. The International Organization for Standardization established a working group to study the expansion of BIN numbers, and it has suggested a move to eight-digit BINs. Currently, the six-digit BIN has two "open slots" (positions seven and eight) for customer relationship management of the cardholders and their transactions, and this would be lost, which would engender a major reengineering that would create system-wide implementation challenges. The real problem is the way that card numbers are allocated and the fact that the existing BIN ranges are not being fully utilized. Currently, there are no immediate plans to adopt this.

PAR Value. When a merchant takes a transaction that has been key-entered, swiped, or as part of an e-commerce/card-

not-present sale, and converts it to a token, it needs to be tied to the original transaction that the consumer authorized. The payment account reference (PAR) value allows the linkage of the cardholder's token with his or her PAN without needing the underlying card number. When a token is created, a PAR value also is created and must be supplied with all future authorization requests. Last year, EMVCo added a new field for PAR, which must be used by acquirers, issuers, and merchants. This means potential changes to terminals, gateways, processing systems, and potentially other integrated solutions. It is projected that a chargeback could be initiated on a transaction without a PAR value because proof of a customer authorization is lacking. Merchants whose payment processor cannot support PAR are at risk of chargeback fees, loss of sale proceeds, and ending up in an excessive chargeback category—pretty scary.

QIR. Qualified integrator and reseller (QIR) is the term used for a Visa mandate requiring small businesses to use only qualified companies or individuals to support PCI DSS compliance. It calls for secure installation and maintenance of validated payment applications that process, store, or transmit sensitive cardholder data. The people who install, support, and maintain payment applications should be certified so as to not introduce any vulnerability in the cardholder data environment. QIR went into effect on Jan. 31, 2017, and, as of then, all Level 4 merchants must use solutions providers with this certification. The issue here is something called "remote access solutions" (RAS), such as Microsoft Remote Access Desktop, which are typically used to provide remote support for small merchants. If a RAS is not securely installed, it creates an access road for a cybercriminal or fraudster, who can then log in, install malware, record keystrokes, capture audio and video from the device, and steal payment card track data. Some ISVs and POS resellers are still not prepared to meet the QIR requirement. The key here is that the installer must use a validated payment application, compliant with the Payment Application Data Security Standard. A directory of qualified providers can be found at www.pcisecuritystandards.org.

To spur compliance [for 2-series BINS]... an acquirer may be subject to monthly fines for noncompliance of up to $25,000, and their small merchant could be fined as much as $100 for accepting a card for a $25 purchase.

In addition, changes are coming in the world of automated clearing house (ACH) payments. ISOs typically focus on card-related payments, and merchants typically look to their bank for ACH processing. I have an Accredited ACH Professional certificate, and I have a pretty hard time interpreting the rules mandated by the National Automated Clearing House Association. Recently, I was trying to figure out whether a transaction over the internet should have a WEB or CCD standard entry class code. I had to call our local experts for a ruling, because neither our attorney nor I could figure it out. I suggest that, for the time being, ISOs and member service providers focus on the changes in the card processing world, and let your merchants leave the ACH processing to their bank or to a qualified third-party processor that specializes in ACH.

As you can see, it is almost a full-time job just keeping up with all the changes mandated by the card brands. ***TT***

Brandes Elitch is director of partner acquisition for CrossCheck Inc.

ADVERTISERS INDEX

Jordan Lampe

As head of strategic projects for Dwolla, Jordan Lampe leads mid- and long-term initiatives for the payment API provider. Since 2015, he as been involved with the Federal Reserve's Faster Payments Task Force, which recently released its final report for achieving a fast payments system over the next three years.

Here, we talk to Lampe about his invlovement with the task force and Dwolla's faster payments solution proposal.

Why did you get involved in the task force?

Prior to building the ideal API for businesses, Dwolla had built what it felt was the ideal API for banks. The protocol, called FiSync, offered the ability to clear and settle funds in real-time and offered instant availability of funds. We felt our first-hand experience could help the task force think through some of the challenges we faced and shine light on the opportunities we saw back in 2012 when we began turning on FiSync at financial institutions. As it turns out, talking about about faster payments with banks was more productive for the conversation than building or integrating an actual system.

I'm proud of the contributions of Dwolla and our nonbank service providers' segment contribution. I firmly believe that, together, we've helped create a thoughtful final report and increased the odds for a new system to take root. And, while that's ironic—as Dwolla no longer actively sells FiSync to banks—it was a worthwhile and humbling opportunity for us to learn, collaborate, and be a part of that.

Personally, I'm fascinated by our current system. Specifically, the challenges and opportunities over time that shaped it. Being involved with the Faster Payments Task Force provided a unique lens to peer into and help influence these conversations in real-time.

What were some of the biggest insights you gained as a member and/or from being on the steering committee?

Honestly, that at the end of the day, [task force members] are all just a bunch of payment nerds. After all, it takes a special kind of person to truly want to geek out and get in the weeds to debate "push payments," payment nomenclature, and system governance. How else to explain why over 300 task force members—probably 20 to 30 percent of whose companies have been named as a defendant by someone else in the room at one time or another—came together to agree on and achieve so much? Sure, there were market forces bringing big brands to the table, but it was a shared desire to be a part of a once-in-a-lifetime opportunity to build the next generation of payments in the world's largest economy that brought about and brokered some of our biggest breakthroughs and compromises.

Dwolla was among the companies that submitted a solutions proposal. Can you briefly describe it?

Our proposal drew from our past and present. For starters, we married our FiSync engine for interbank clearing and settlement with our current flagship product, called the Access API. Today, the Access API provides a simple yet sophisticated directory, ledger, settlement system, and banking relationships to businesses so they can connect to the existing ACH system. Combining these two created a holistic, end-to-end vision for how a modern payment system not only would operate at an operator level, but how financial institutions and nonbank services providers could use APIs to help monetize and broker access to a faster payment system.

Given the scope of the initiative and the complexity of the U.S. payments ecosystem (not to mention no mandates for enforcement), would you describe the goal of a faster/better payments system by 2020 more aspirational than obtainable?

It's absolutely attainable. The task force represents hundreds of stakeholders from eight different segments, ranging from small banks to consumer groups. In other words, the task force represents the market. That realization provides many key decision makers, both at the Fed and bank level, with the necessary buy-in to take action on things like a real-time gross settlement system at the Fed or fulfill our requests for guidance on regulatory oversight.

These larger institutions, organizations, and agencies need this system as much as payment geeks want it. This final report, in no uncertain terms, gives them the clear guidance to take action.

The report is out, so what's next for you and your work on the task force?

One of the biggest challenges lies in establishing the framework for how the market (i.e., "us"), policymakers, and the Fed will govern and standardize these systems in the future. These were two obvious "gaps" we identified among the 16 proposals that we knew needed continued leadership on in the coming months. While I've stepped back a bit from leadership responsibilities, we have a great mix of new task force members and existing steering committee members leading this temporary group, called the Interim Work Group Committee.

I will continue to stay close to the effort. We have big plans for Dwolla and faster payments. ***TT***

ACCELERATE BUSINESS | AMPLIFY VOICES | EXPAND KNOWLEDGE

YOUR ETA: NOW

Cayan now has a 75,000-customer base with the help of ETA.

ETA has helped us build our business over the past 15 years. From the business relationships and the advice we get from other members year-round, we've learned the inner workings of the industry and have seen the future. There really is no other resource for our industry like ETA.

Henry Helgeson, CEO and Co-Founder, Cayan

ETA
ELECTRONIC TRANSACTIONS ASSOCIATION
Advancing Payments Technology

ELECTRAN.ORG

Experience the value of ETA Membership and arrive at a greater level of success. Join today.

We didn't make a $2 million commerical and you still found our ad.

We focus on results, not flash.

We provide agents and ISOs with the latest tools, products and resources to help *get* ***more*** customers, and ***keep*** them longer.

Contact us to learn how we can help build your business.

(Or if you're considering a $2 million commercial)

iPayment®

Learn more at **iPaymentInc.com**