DIGITAL TRANSACTIONS

Trends in the Electronic Exchange of Value

THE SURGING ACH

The big, 46-year-old network, with links to virtually every bank in the country, is on a growth tear. **Here's why.**

Volume Seventeen, Number Four • DigitalTransactions.net • April 2020

ALSO IN THIS ISSUE:

contents

APRIL 2020 • VOLUME 17, NUMBER 4

Cover Illustration: Jason Smith, 123RF.com

Digital Transactions (USPS 024-247) is published monthly by Boland Hill Media LLC, 800 Roosevelt Road, Building B, Suite 212, Glen Ellyn, IL, 60137. Periodicals Postage Paid at Glen Ellyn, IL, and at additional mailing offices. POSTMASTER: Send address changes to Digital Transactions, P.O. Box 493, Northbrook, IL 60065-3553.

MAGTEK®
SECURITY FROM THE INSIDE

Empowering the Consumer Journey in the Branch of the Future

with mobile in-branch hardware, flexible software and secure services.

MagneSafe®

This security architecture safeguards your environment with a layered approach of encryption, authentication, tokenization, and dynamic data

Versatility

DynaPro Go is a secure mobile PIN PED that provides convenience, accepting a variety of payment and ID methods in the market today.

Authentication

Increase confidence with layers of security. Multi-Factor Authentication minimizes risk and offers peace-of-mind.

Increase Consumer Engagement

Surpass expectations and go beyond the teller line with faster more engaging solutions, accessing protected and encrypted account information in the palm of your hands.

FIND OUT MORE

562.546.6467
sales@magtek.com
www.magtek.com

MagTek, Inc., 1710 Apollo Court, Seal Beach, CA 90740

the gimlet eye

THOUGHTS IN THE TIME OF PLAGUE

AT THE TIME OF THIS WRITING, a plague has descended on the world, and it's not likely to have lifted by the time you read this column. Covid-19, a novel form of the coronavirus, originated in China this winter but has now swept through countries around the globe, sickening and killing thousands.

The impact on multiple industries has been heavy. In the United States, restaurants and bars in many states have been forced to close by state or local edict, leaving them with only their delivery and takeout businesses. Other firms have sent their workers away to work at home in the interest of slowing the virus's spread, doubtless a wise move but one that in its own way takes a toll on local businesses as people avoid crowds.

In the face of these wrenching changes and the downright suffering the virus has caused, it seems gauche somehow to consider the toll the plague has taken on payments. But payments is a business, and this is a magazine that covers that business. So consider we must.

But in the wake of registering the impact on consumer spending, on the payment media used for that spending, and the fortunes of this or that technology, can we lose sight of the very real human cost of this pandemic? Too often, we think, this dimension has been lost in the flood of coverage, overtaken by the speculation on, say, whether contactless payment will win out at the point of sale because it doesn't require the user to touch that filthy point-of-sale device.

We plead guilty. We've run such stories. So have our competitors. But modern medicine will ultimately defeat this plague. Businesses and payments will rebound. And we'll have a market verdict on whether contactless payment has become habitual. Then, with all the questions about the virus having been answered, the devastation remembered, the final costs toted up, the altered and ended lives lamented, what will really matter? That some payment method, some API or SDK, emerged with momentum, smiled on by merchants, consumers, and payments impresarios?

Will we remember the cost in human terms? A strange question for a business publication to ask, yes, but we think it would be a deeply sad thing to lose sight of what it gets at. It would be yet another casualty of the plague to recall, when it finally subsides, not the toll it took on our family, friends, or colleagues, but rather the way it reshaped this or that business practice, how it favored or disfavored this or that technology.

Now, while the virus rages, let's resolve not to let that happen.

John Stewart, Editor | john@digitaltransactions.net

APRIL 2020 • VOL. 17, NO. 4

DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

PUBLISHER Robert A. Jenisch

EDITOR-IN-CHIEF John Stewart

SENIOR EDITOR Jim Daly

SENIOR EDITOR, DIGITAL
Kevin Woodward

CORRESPONDENT
Peter Lucas

ART DIRECTOR/PRODUCTION EDITOR
Jason Smith

DIRECTOR OF ADVERTISING
Robert A. Jenisch, 877-658-0418
bob@digitaltransactions.net

ADVERTISING SALES REPRESENTATIVES
Robert Mitchell, 877-658-0418, x7
bmitchell@digitaltransactions.net
Rob Akert, 877-658-0418, x6
rakert@digitaltransactions.net

Digital Transactions, *Digital Transactions News*, and DigitalTransactions.net are publications of Boland Hill Media LLC, 800 Roosevelt Road, Suite B212, Glen Ellyn, IL 60137

John Stewart, Managing Director
Robert A. Jenisch, Managing Director

For advertising information, call 877-658-0418. To subscribe or give us a change of address, go to www.digitaltransactions.net and click on "Subscriber Care" or call 847-559-7599.

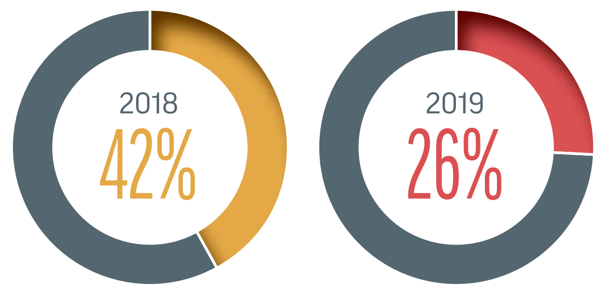
Subscription prices: $59/year for subscribers in the United States; $69/year for Canadian subscribers. All other subscribers, $119/year, payable in U.S. currency.

BPA WORLDWIDE

PCI COMPLIANCE IS GETTING TOUGHER

A QUICK EROSION IN COMPLIANCE

(Portion of payments providers reporting 60% or more of merchants in compliance with PCI)



Source: ControlScan/MAC 2020 Acquiring Trends Report

Independent sales organizations are increasing their use of non-compliance fees for merchants that don't adhere to PCI Security Standards Council requirements, with 23% of ISOs surveyed for the ControlScan/MAC 2020 Acquiring Trends Report saying they assess these fees. That's up from the historic range of 17% to 18%.

The report, released in March, is based on a survey last fall of 68 payments-industry professionals.

Only 26% reported compliance rates above 60%. It had been 42% in 2018. The reasons for the drop are multiple, but chief among them—with 50% citing it—is that merchants were initially compliant, but their annual validation lapsed.

Another factor, at 20%, is the decreased frequency of communications about compliance. Other factors—at 10% each—include a change in PCI-compliance program partners, decrease or elimination of merchant education on compliance, decrease or elimination of noncompliance fees, and more complex compliance requirements.

"When combined with regular communications and educational content, scope-reducing technologies and related services are a powerful way to make life easier for the merchant," said Chris Bucolo, ControlScan vice president of market strategy, in a statement. "It's all about giving the merchant the tools and support they need to properly secure their business, without overburdening them."

The survey data, which focused on payments providers serving small and mid-size merchants, also highlights that successful PCI-compliance programs are not set-and-forget, he says. "Running a successful PCI-compliance program requires regular reviews of metrics and trends so that corresponding adjustments can be made," said Bucolo. "Like security technologies, there is no 'set and forget'."

Though PCI noncompliance fees have a role, of those that don't charge these fees, many—77%—said they opt not to because of strategic and competitive purposes. Twenty-three percent said the fees don't increase compliance rates.

Many ISOs try to motivate merchant compliance by using a third-party service provider, increasing merchant education, increasing the frequency of communication about compliance, and reducing or waiving PCI program fees for compliance, among others, according to the survey results.

Atlanta-based ControlScan and the Merchant Acquirers' Committee, an association of payment-risk professionals, sponsored the survey.

—Kevin Woodward

RANSOMWARE'S HEAVY TOLL ON THE PUBLIC SECTOR

As the plague of ransomware continues to roil digital payments and other industries, it turns out state and local governments are proving to be particularly vulnerable.

RANSOMWARE'S TOLL	Average Payment	Average Downtime
	$84,116	16.2 days

Source: Coveware

In fact, ransomware attacks on school systems, police departments, city administrative offices, and other governmental agencies are rising fast. Last year, state and local entities reported 163 attacks costing more than $1.8 million in ransoms paid, according to a report released last month by the consulting firm Deloitte & Touche LLP. That number of attacks was up 150% over the number tracked in 2018, the firm says. The total cost of recovering from these incidents amounted to "tens of millions of dollars," says the report.

Indeed, attacks on public-sector units accounted for fully 10.4% of all cases tracked in the fourth quarter of last year, according to Coveware Inc., a Westport, Conn.-based cybersecurity firm.

In a number of cases, principled refusal to pay has turned out to be the more expensive option. The city of Baltimore, for example, last year refused to pay $76,000 demanded by cyber criminals who had locked up its systems, but then faced $18 million in recovery costs and foregone revenues.

In a typical ransomware attack, perpetrators don't steal data. Instead, they use encryption software to scramble the data and then demand payment for the encryption key. Now, in a new twist, perpetrators are starting to pull the locked data into their own systems and threatening to release it publicly if they aren't paid, according to a report Coveware released in January. Typically, the criminals demand payment in Bitcoin.

But why are attacks on the public sector increasing? Deloitte cites several reasons. For one thing, government entities usually perform routine but vital functions whose interruption could bring inconvenience, if not harm, to ordinary citizens. That makes these entities more vulnerable and raises the likelihood that they'll pay up, the report says.

Another issue lies in what Deloitte calls an expanding "attack surface." Every police car and classroom is likely to have a computer in it, says the report, adding that system-linked traffic cameras, ambulances, trash haulers, parking meters, and libraries add to the range of vulnerable attack points.

But perhaps the biggest issue is that strained budgets mean much technology used by local governments is outdated, leaving them without the patches and other protections usually found in private-sector systems. "For state and local governments operating with older, legacy systems, keeping those systems up to date can be a daunting battle," says the Deloitte report, entitled "Ransoming Government."

To this mix, the report adds the rising importance of cyber insurance policies, which can make governments more likely to pay ransoms because the payouts cover all or much of the demand. In the second quarter last year, governments that paid ransoms shelled out 10 times more than what was paid by private-sector victims, says Deloitte.

"Cyber insurance, poor defense, and criticality of government services are creating a positive feedback loop where attackers are asking for and getting more money more often," according to the report.

To fight the trend toward more attacks and higher ransoms, Deloitte recommends governments take steps to isolate critical data in ways that wall off the information from other areas of the system that might come under attack. It also advises steps such as making security patches a priority and running simulations, or "war games," to prepare staff for attacks.

—John Stewart

$50 MILLION ON THE SPOT

Fast-growing payment technology and software provider SpotOn Transact Inc. in March raised $50 million in a Series B funding round that included 01 Advisors, an investment firm led by three former Twitter Inc. executives.

SpotOn, which says its revenues increased by more than 150% in 2019, will use the funding for product development. The company provides business-management software and payment services to small and mid-size businesses, including restaurants, and is a registered independent sales organization for Merrick Bank. Last June, San Francisco-based SpotOn announced a $40-million funding round.

01 Investors was founded by Dick Costolo, Twitter's former chief executive, and two other veterans of the social network, Adam Bain, the ex-chief operating officer, and David Rivinus, the former corporate-development and investor-relations executive. The newly announced investment was their first in SpotOn, which SpotOn president RJ Horsley says has raised a total of $130 million since its 2017 founding.

"There are companies that build great products, and there are companies that build great sales teams, but it's rare to find an organization that can do both," Costolo, 01 managing partner, said in a statement. "SpotOn has proven an unwavering commitment to building products that matter and getting them into the hands of businesses nationwide."

Twitter is headed by Jack Dorsey, who also is chief executive of Square Inc., a processor and software provider that competes for small-business clients in some of SpotOn's same target industries.

SpotOn, which said it has added 5,000 clients in 2020 alone but didn't reveal its total merchant count or payment volume, was founded by twin brothers Matt and Zach Hyman along with Chicago fintech entrepreneur Doron Friedman. The Hyman brothers sold their remaining 15% stake in the ISO they founded, Central Payment, to Total System Services Inc. (TSYS), now part of Global Payments Inc., in a 2018 deal that valued Central Payment at $840 million. TSYS and Central Payment first formed a 60-40 joint venture in 2012.

Other participants in the recent funding round included returning investors Dragoneer Investment Group, Franklin Templeton, and Epiq Capital Group.

—Jim Daly

Photo: Web Summit

Costolo: "There are companies that build great products, and there are companies that build great sales teams, but it's rare to find an organization that can do both,"

COVID-19'S BOOST FOR CONTACTLESS PAYMENTS

The coronavirus pandemic has prompted a number of warnings that could end up benefiting electronic payments, particularly contactless transactions.

Authorities ranging from the World Health Organization to doctors in local practices have warned about the risks of handling paper currency, and some have also cautioned against touching publicly available terminals used for everyday interactions, such as point-of-sale devices and ATMs.

Now, payments experts are talking about a positive impact for technology that allows consumers to avoid touching bank notes or devices in stores or other public places.

"Someone approached me at our conference [in February] and suggested that we should be talking about the benefits of contactless and [near-field communication] as a more sanitary means of making payments transactions," notes Randy Vanderhoof, executive director of the Princeton Junction, N.J.-based Secure Technology Alliance. The STA's annual conference took place in Salt Lake City.

A letter from a doctor that appeared in *The Wall Street Journal* last month warned not only against Covid-19, the coronavirus strain spreading from country to country, but also against flu and other

State and local authorities in March began ordering restaurants to close, allowing only takeout and delivery orders.

viruses. He advised that "the rapid implementation of contactless credit card devices ... would be cost-effective and help to prevent the spread of many viral infections..."

As Covid-19 spreads, causing state and local authorities to mandate restaurant closings and other actions to encourage so-called social distancing, will the disease prompt more contactless installations?

Visa Inc. reported in January that one-third of its card-present transactions worldwide are contactless, up from a quarter a year ago. And while the contactless share in the U.S. market is much lower, some extensive mass-transit agencies, including New York City's Metropolitan Transportation Authority, are launching systems that accept general-purpose contactless credit and debit cards.

Whether the virus scare will prove to be a lasting boon for technologies such as contactless POS devices remains to be seen, but some observers contend it could well provide at least a short-term boost. "Contactless cards and mobile NFC are much safer because they do not come in contact with the reader and no one else needs to handle the card in most cases," says Vanderhoof in an email message.

Vanderhoof points out that even more recent technologies like contact EMV don't provide the same protection. "Using EMV dip readers means that even if no one else handles my card, I am [potentially] getting transfer germs from the other cards that were inserted into that device," he warns.

Contactless, though, isn't always contact-free. In some circumstances, consumers using debit cards can be prompted to enter a PIN, requiring them to touch a keypad or device screen. PIN entry is usually governed by network or issuer rules. Vanderhoof said he did not have data on the percentage of contactless debit transactions requiring a PIN.

And the ripple effects of the Covid-19 scare could work against some payments technology. ATMs, for example, are typically used to dispense cash, a medium some experts have cautioned can spread the disease. The WHO, an agency of the United Nations, has warned that bank notes can remain infectious for a number of days, and advised users to wash their hands after handling them.

So far, though, experts aren't seeing an impact on ATM activity. "I haven't heard anything from any of our members on this," says David Tente, executive director, USA and the Americas, at the Sioux Falls, S.D.-based ATM Industry Association. "Our members at this point aren't expressing any concern."

—John Stewart

ANT BUYS A STAKE IN KLARNA

Klarna Bank AB, a leading exemplar of the trend toward offering installment-plan payments online and at the point of sale, received backing from Ant Financial Services Group in a March deal that cements an existing alliance between the two companies and could add considerable propulsive force to Klarna's relatively new consumer app.

China-based Ant, parent of the hugely popular Alipay mobile wallet, and Klarna announced that Ant has bought an unspecified "minority stake" in the 15-year-old unicorn. Citing a Klarna spokesperson, CNBC reported at the time of the announcement that Ant's position comes to "less than 1%" of Klarna's equity. A unicorn is a privately held company with a valuation of $1 billion or more.

Ant's move results in a much closer relationship between the two companies, which are already cooperating on payments. Shoppers on AliExpress, for example, can use Klarna to make installment payments. AliExpress is a global e-commerce site owned by Alibaba Group, of which Ant Financial is the payment arm.

Peterson: "Buy now, pay later is a rapidly expanding category in digital commerce and Klarna is one of the global leaders."

The tighter relationship also comes just 10 months after Klarna's introduction of an app that allows users to pay merchants online without leaving the app. Users make four equal payments, paying the first installment immediately and the other three at two-week intervals. The number of downloads is now 33 times that seen in May, Klarna says, without giving a specific number.

Installment payments at the point of sale have gained considerable attention in the last couple of years as merchants and payments companies seek ways to open online and in-store payments to a broader cross-section of consumers. Mastercard Inc., for example, in April acquired Vyze Inc., a prominent startup in the business. Other competitors include Affirm Inc., which a year ago clinched a deal to support installment payments at Walmart Inc.

"Buy now, pay later is a rapidly expanding category in digital commerce and Klarna is one of the global leaders," says Thad Peterson, a senior analyst at Aite Group.

Now, with Ant's ownership stake, both companies stand to benefit beyond what they might have expected from their cooperative agreements, Peterson says. "The deal offers the potential of significant expansion for Klarna," he notes in an email message. "The combination of Alipay and Klarna dramatically increases Klarna's global footprint and adds millions of potential customers. For Alipay, adding Klarna enhances the value proposition for their payment offering and further legitimizes Alipay as a global payment alternative."

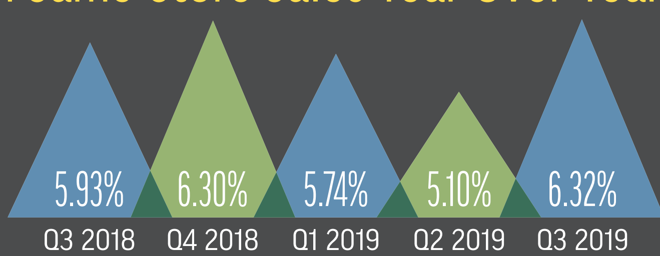
As things stand, Klarna is accepted at more than 200,000 merchants and e-commerce platforms, with more than 75,000 having been added last year, the company says, adding that some 85 million consumers use Klarna. DT

—John Stewart

MONTHLY MERCHANT METRIC

Growth in Same-Store Sales Year Over Year

Annual volume change/growth of retained (non-attrited) accounts for given period divided by total portfolio volume from same period of the prior year.



Note: This is sourced from The Strawhecker Group's merchant data warehouse of over 3 million merchants in the U.S. market. The ability to understand this data is important as small and medium-size businesses (SMBs) and the payments providers that serve them are key drivers of the economy. All data are for SMB merchants defined as merchants with less than $5 million in annual card volume.

Payments Experts. Powerful Data. THE STRAWHECKER GROUP

PAYMENTS IN A TIME OF CRISIS

BY GIDEON SAMID
gideon@bitmint.com

"SOCIAL DISTANCING," the idea that we can slow down the spread of the novel coronavirus by isolating ourselves as much as is practicable, could help fight the disease but may also have bad knock-on effects of its own. It could shut down restaurants and other socially minded businesses, causing layoffs and lack of cash for necessities, leading to civil unrest. More and more entertainment and crowd-intensive businesses may be brought to a screeching halt. People who work at these places could be left with no income.

An untold number of those laid off will be living from paycheck to paycheck. When they cannot feed their kids, they may take action, putting the civil order in jeopardy.

Initial proposals to deal with this include easing taxation and deferring mortgage payments. But these measures are too slow and too slanted against the most vulnerable. Some economists propose an injection of cash focused on those who need it most. Alas, as we know, a spigot of cash is a gold mine for fraud and abuse. In the Iraq war, when Saddam Hussein's regime collapsed, the U.S. government spread around bundles of $100 bills, producing little relief.

Today we have digital-money technology. Smart phones are ubiquitous, and tethered-money technology is well developed (see my book, *Tethered Money,* published by Elsevier).

Whether or not blockchain is an effective money-transmission solution, this crisis shows that the power to mint money, inject money, and redeem money is best handled through the authority that manages the crisis itself. Centralized digital payment can be directly distributed to individual phones. The funds can be marked "emergency money," which is minted as a means to contend with the crisis, and will have to be redeemed against normal currency when the crisis is over.

Here, the full power of identity-bearing digital money comes into play. Any solution where the digital expression carries both value and identity (as, for example, with BitMint) is a solution where the money per se can be cryptographically tied to any logical terms.

An example is range of use. Tethered digital money can be limited to necessities. A differently marked coin will only buy meds, say. Digital coins will carry their chain of custody, and when redeemed will allow the authorities the means to monitor the community and spot individuals in need of help. For example, if an elderly patient living alone fails to buy his meds, the authorities would get a warning signal and a public health official can pay a visit.

Digital money can be injected in small, frequent, measured doses. It may be posted on peoples' phones on Monday morning and lose its value a few days later to inhibit hoarding and abuse.

What is needed without delay: Allocate a tiny portion of funds directed by Congress to fight the coronavirus to commission any credentialed centralized digital-money solution builder to design, build, and test a working solution for the task of phone-injected crisis survival cash.

Let every digital-payment solution with a reasonable prospect for efficacy be funded in parallel, so that. should this crisis follow some of the most alarming epidemiological models, we as a society will have effective tools to quell civil unrest and find a quick path to recovery.

The ultimate victory in this coronavirus crisis is in the hands of physicians and biochemists. But we in the payment industry have a vital role to play to maintain social order. Let's together as a professional community rise to the challenge. Smart and smooth payment systems are among the underpinnings of social tranquility, and we are the custodians of those systems. We should step up. DT

FINTECHS' REGULATORY GRAY AREAS

BY BEN JACKSON
bjackson@ipa.org

THE RAPID GROWTH OF PAYMENTS TECHNOLOGY has created gray areas in regulatory compliance and consumer protection, and regulators are working to catch up.

The most recent example is the request for information published Feb. 26 by the Federal Deposit Insurance Corporation. The FDIC wants comments on "potential changes to its sign and advertising rules to better reflect how banks and savings associations are transforming their business models to take deposits via physical branches, digital, and mobile banking channels." It also asks for input on addressing possible misrepresentations by nonbanks about FDIC insurance.

This request is a recognition that the way money flows in and out of banks has changed, and will continue to change, as new channels open. It also reflects a need for clarity about what companies actually are. Companies that are described as "challenger banks" by themselves or by the press are not federally insured deposit institutions. The deposit insurance that protects their customers is provided by a partner FDIC-insured institution. These third parties are program managers like the program managers in the prepaid card business that assemble value chains to deliver financial services to consumers.

That value-chain structure means the FDIC is not the only regulator that needs to figure out how to move new payments companies out of regulatory limbo. The Consumer Financial Protection Bureau created a large gray area when it finalized its prepaid-accounts rule in October 2016.

First, the CFPB did not limit its rule to prepaid cards. It said digital wallets "to the extent that they are used to access funds the consumer has deposited into the account in advance" should be covered by the rule. It also specified that the access method is not what's at issue, but rather that an account exists.

However, the CFPB then complicated things when it said that "the Bureau declines to limit coverage under the definition to accounts held in a pooled account structure, because the Bureau believes that the characteristics that make an account a prepaid account should not be dependent on the product's back-office infrastructure." Rather, it was more concerned with "the way the account is marketed or labeled, as well as ... the account's primary function."

With account structure set aside, it seems that compliance depends in part on good marketing. If a fintech wants to avoid the strictures of the prepaid rule, it appears it will likely market itself as a "different" kind of bank account, or least not as a prepaid account. But, as the FDIC's request demonstrates, these companies are not banks themselves.

Regulators face two important questions. First, if fintechs are not banks and not prepaid accounts, then what are they? More important, what recourse do their customers have if something goes wrong?

These questions will be at issue in the lawsuit PayPal filed against the CFPB in December. PayPal argues that its digital wallet should fall outside the scope of the prepaid rule because digital wallets are fundamentally different from prepaid accounts. It also argues that the rule's requirements for disclosures are unconstitutional because they violate the First Amendment.

It might be easy to see the suit as something that primarily concerns PayPal. But if PayPal succeeds, it is likely that the rule itself will be thrown out. This would mean that the payments industry would go back to where it was in 2012—being regulated under a patchwork of agencies and rules, with no guiding principles. It also could mean that consumers would see account protections become contractual instead of codified.

Regulators will need to resolve this fintech regulatory limbo to protect both the banks that make these products possible and their customers. DT

A CLOUDY FORECAST

It seems there's nothing hazy about the future of cloud-based POS. What's driving the trend?

BY **PETER LUCAS**

CLOUD COMPUTING IS A PART OF DAILY LIFE. Whether it's banking online, making a P2P payment, streaming movies on a smart television, or sending an email (think Gmail), most software applications, data storage, and networking capabilities are delivered through remote servers via the Internet.

Driving the popularity of cloud computing is the cost efficiency of its infrastructure, which eliminates the capital expense of on-premise servers and enables remote maintenance capabilities and on-demand scalability to meet changing user needs.

Thanks to mobile devices, which allow access to apps anywhere, any time, cloud computing has become so ubiquitous consumers rarely give it a second thought.

Merchants, on the other hand, are a different story. With the exception of a handful of merchant categories, such as restaurants, merchants remain tethered to the traditional notion of point-of-sale system infrastructure, running applications off, and storing data on, a local server. This despite their comfort using cloud-based services in their personal life.

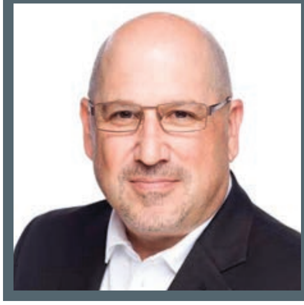
Merchants' dated perception of POS systems has not only slowed their adoption of cloud-based technology, but made the technology a harder sell, because the less merchants understand about a new technology, the more inclined they are stick with what they know.

"Even though cloud-based technology has been around for years, cloud-based POS systems are still a bit too complicated for many merchants to understand," says Ken Schember, vice president of mid-market, ISO and VAR Solutions for payment solutions provider PAX Technology Inc.

As a result, cloud-based POS systems are just beginning to percolate to the surface as independent sales organizations and value-added resellers alter their sales strategies to better educate merchants about

the benefits of cloud-based POS systems, Schember adds.

A big selling point is affordability. The total cost of ownership for a cloud-based POS system can range up to 20 times less than a traditional POS system, payments experts say. On average, a single, traditional POS system can run between $3,000 and $7,000 to install, plus hundreds of dollars in monthly service fees. Merchants installing multiple POS terminals can expect to spend tens of thousands of dollars, if not more.



'There is really no need for onsite installation or laying cable with cloud-based systems. That reduces a lot of upfront costs.'

—PAT WARD, VICE PRESIDENT, INTEGRATED AND ENTERPRISE SALES, NORTH AMERICAN BANCARD

Those costs do not include the price of on-premise servers, which are essentially a rack of computer hardware for capturing data, processing transactions, and generating analytical reports on sales performance.

"An on-premise POS system can be five to 20 times more expensive than a cloud-based POS system if you factor in hardware, maintenance, software, and licensing fees," says Anthony Zhang, vice president of sales for payment technology provider Fattmerchant, Inc.

TIGHT BUDGETS

The emphasis on price as a key selling point for cloud-based systems is not surprising, as cost has always been a big consideration for merchants when it comes to upgrading their POS systems. That's especially true for small and medium-size merchants on tight IT budgets.

Factors contributing to the affordability of cloud-based POS systems include ease of set-up, the option for merchants to purchase generic hardware that can interface with legacy back-office systems (such as tablet computers rather than a proprietary terminal), and automatic, remote software installation and updates.

"There is really no need for onsite installation or laying cable with cloud-based systems," says Pat Ward, vice president, Integrated and Enterprise sales for North American Bancard. "That reduces a lot of upfront costs."

Plus, cloud-based systems typically charge low monthly subscription fees that include maintenance, making it easier for merchants to budget for the technology.

Toast Inc., a provider of POS systems for restaurants, charges between $79 and $150 per month for its software, for example. In addition, Toast charges $100 per hour for onsite support and $400 to build a full menu in the merchant's POS system.

A lower cost of ownership and ease of installation make it easier for merchants in need of replacing aged, legacy POS systems to embrace cloud technology.

CHANGING DEMANDS

So far, restaurants have been on the leading edge of adoption because of myriad changes in how their industry services customers.

Third-parties such as Uber Eats make it possible for restaurants to offer online food ordering and delivery. In addition, sit-down restaurants have begun equipping wait staff with tablet computers that can accept orders and payment at the table. The latter helps increase table turnover by speeding payment, which can increase a restaurant's revenues, not to mention customer satisfaction, payments experts say.

Such advances have led restaurants to conclude their existing POS systems need to be upgraded to handle these new functions, which has made them more open to new POS technology.

"As a restaurant operator, if you're going spend the money to upgrade your existing POS system, you might as well spend it on new technology that can keep up with the changing demands restaurants are placing on their POS systems," says Chris Lybeer, chief strategy officer for Revel Systems, provider of a cloud-based POS system. "Traditional POS systems can't support processing orders at the table or accepting orders online."

Accepting payment at the table through a tablet computer is also easier for wait staff and customers than through a hand-held POS terminal, Lybeer adds.

As part of its POS system, Revel, which focuses on servicing


EVO

restaurants and specialty merchants, offers restaurants a white-label application to accept online orders. "This eliminates the service charges levied by third-party providers," Lybeer says.

Other POS systems providers vying for a slice of the restaurant industry include Toronto-based TouchBistro Inc., New York-based ShopKeep Inc., Montreal-based Lightspeed, San Francisco-based Square Inc., Providence, R.I.-based Upserve Inc., and Sunnyvale, Calif.-based Clover Network Inc., a division of Fiserv Inc.

With the cloud, 'merchants can update inventory or change pricing remotely.'

—MARK SCHULZE, VICE PRESIDENT, FISERV

BEYOND LOWER FEES

While cost can be a big selling point for cloud-based systems, ISOs are discovering merchants often need to be educated about how the technology can benefit their businesses before they will move away from traditional credit card readers and electronic cash registers. In other words, sales reps can't sell a merchant on cloud technology simply by offering to cut transaction fees.

Instead, ISOs should emphasize that cloud-based systems can also run business applications, such as inventory management and time and attendance, that can make the POS system a center for managing their business.

"The remote log-in capabilities of cloud-based systems means that merchants can update inventory or change pricing remotely, which is a big benefit, because the merchant is no longer tied to their system onsite," says Clover co-founder and Fiserv vice president Mark Schulze.

Other education tools being used by ISOs include webinars, testimonials, and old-fashioned sales presentations that walk merchants through the benefits of the technology.

"To market cloud-based POS systems, you still need to speak in a language that the merchant understands," says Fattmerchant's Zhang.

The goal, Zhang adds, is to take a consultative selling approach by demonstrating system parity with on-premise POS solutions, then highlighting the added functionality cloud-based systems can provide beyond what traditional POS systems offer. For example, the open application programming interfaces common to cloud-based systems can provide better connectivity with back-office solutions than a traditional POS system.

Remote access also allows POS-system providers to log onto a merchant's device, with the merchant's permission, and walk him through how to troubleshoot problems and reboot the device. Hence, most issues can be addressed by a dedicated customer-support manager, or fixed by the development team that runs the cloud-based POS solution, on a remote basis. Software companies, such as Microsoft Corp., already offer this service for consumers.

Another check in the plus column for cloud-based POS is that updates can be received automatically across all devices.

What sales representatives want to avoid when marketing cloud-based POS is trying to create a new category or niche for their solution, Zhang says.

Data security is another sticking point when it comes to selling cloud-based systems. Many merchants fear that because data is transmitted via the Internet to a remote server, it is more vulnerable to hackers than data stored in an onsite server.

Debunking those fears starts with pointing out that card data moving through cloud-based POS systems is encrypted and that merchants don't hold the keys to encrypt and decrypt the data, payments experts say.

MagTek Inc., for example, offers a gateway compatible with cloud-based POS systems that encrypts and decrypts transaction data on the front end and back end, respectively. The encrypted data is replaced with a token, which turns meaningful data into a string of random characters that have no value to criminals should the server or network be breached.

"There are scare tactics out there when it comes selling cloud-based POS systems, but with so much of what we do technologically today taking place in the cloud, it should not be hard to educate merchants

about data security in the cloud," says Lybeer. "Merchants should not be running client-server solutions in today's technology environment."

'Merchants should not be running client-server solutions in today's technology environment.'

—CHRIS LYBEER, CHIEF STRATEGY OFFICER, REVEL SYSTEMS

'THE NEXT WAVE'

With the buzz around cloud-based POS systems growing, payments experts predict merchants across more categories will begin adopting the technology for its low cost, user friendliness, and ease of maintenance. "Merchant demand for the technology is growing, and there are more developers pushing into this space," says John Arato, vice president and general manager, retail solutions, at MagTek.

One merchant segment likely to be slower to adopt the technology, however, is large chains. The reason, payments experts say, is large merchants tend to be the most heavily invested in their legacy systems, which can create more hurdles in developing the business case for a full-scale replacement.

"The big chains will likely be the last to get on board, because the investment in their enterprise systems is so great, it makes rip and replace a heavier lift," Lybeer says. "We see specialty merchants and service-based merchants as the next wave."

In the meantime, expect the noise about cloud-based POS to continue to rise as more merchants with firsthand experience become evangelists for installing it. "Merchants I talk to rave about the technology's cost effectiveness, ease of use, and flexibility," says Arato. "We see a lot of growth ahead for cloud-based systems." DT

TRANSIT PAYMENTS IN TRANSITION

Public-transportation fare payments are morphing from closed-loop magnetic-stripe cards to contactless cards and mobile payments. Up next: One app to pay for all, including scooters, bikes, and shared rides.

BY JIM DALY

(Photo: Marc A. Hermann / MTA New York City Transit)

TOKENS ARE LONG GONE and magnetic stripes are going. Contactless is coming. Beyond that, one app for all?

That, in a nutshell, is the state of fare payments for public transportation in 2020. All the while, cash is being relegated to a mandatory but decreasing role as a payment option mainly for riders who have no access to cards or mobile apps, or just don't care to use them.

Now transport officials are abuzz over the idea of just one payment for a multi-leg trip from different providers—from parking at the local commuter-train stop to the train fare itself to a ride on a rented scooter or bike from the downtown station to the office—all compiled and mapped out through a payment-enabled mobile app.

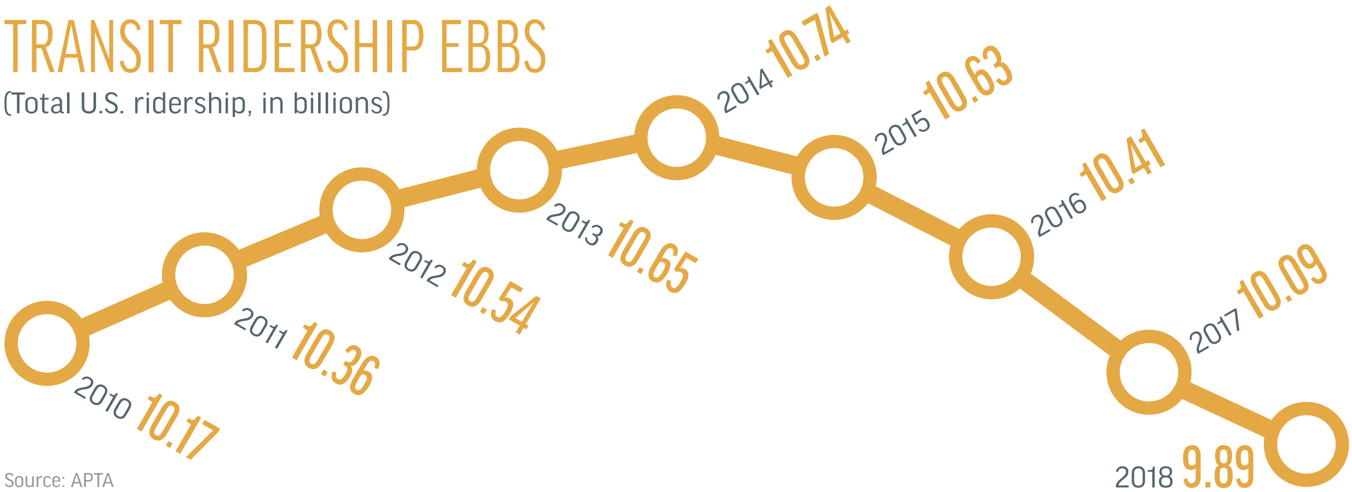
It's a concept dubbed mobility as a service, or MaaS, and in its fullest expression it involves both public- and private-sector transportation providers.

Transit managers, software developers, and consultants in the payments and passenger-transportation industries have been talking about MaaS for several years. Now, it's gaining some traction, though it'll be years before it reaches widespread adoption.

Still, the idea is intriguing.

"We know there are all of these competing and complementary modes of service," says Randy Vanderhoof, executive director of the Princeton Junction, N.J.-based Secure Technology Alliance and director of its affiliate, the U.S. Payments Forum. "The consumer doesn't care. They just want to get from Point A to Point B."

The STA held its annual Payments Summit in late February. The Salt Lake City conference included considerable content about transit-



fare technology, with MaaS getting a lot of attention.

"We're definitely headed in that direction," says Jeff Hiott, vice president of technical services and innovation at the Washington, D.C.-based American Public Transportation Association.

SLIPPING RIDERSHIP

Apart from MaaS, the public can see concrete evidence of technological advancement in fare payments with the coming of proprietary media and acceptance of open-loop contactless cards—debit or credit cards with a Visa, Mastercard, American Express or Discover logo—and mobile payments on many systems.

Some 20% of the nation's transit systems are now capable of accepting open-loop payments, according to APTA. The Chicago Transit Authority has accepted them for several years, and now some other big transit markets, especially New York City's Metropolitan Transportation Authority, are getting on board.

While they're further along than MaaS, open-loop payments still have miles to go before they can claim a big share of payments. Percentage-wise, open-loop's share is probably in the low single digits.

Nonetheless, transit officials say they must play the long game and prepare for MaaS even though many systems haven't yet completed replacements of 1990s-era mag-stripe cards. That's because the huge growth of alternatives—everything from ride-share firms such as Uber and Lyft to services that let you rent a bike or scooter through a mobile app—has changed the transportation game.

Transit is struggling to keep riders in this new era of multiple options and cheap gas. According APTA, annual public-transportation ridership reached a recent peak of 10.7 billion in 2014, then slipped each year afterward to 9.89 billion in 2018 (chart).

Final 2019 ridership data were unavailable at the time of this article, but APTA figures for the year's first nine months show an increase of less than 1% over the same period in 2018, to 7.4 billion.

MaaS is more developed in such European cities as Helsinki, Vienna, and Hamburg, according to Rupa Krishnan, vice president and head of network products at American Express Co. and a speaker at the STA's conference. In the U.S., MaaS needs a partnership between the public and private sectors to take off, she said in her presentation, adding that governments may need to enact enabling legislation, and all parties need to commit to data sharing.

"The key role played by the public sector in implementing MaaS cannot be [underestimated], especially in cities where commuters depend on public transit to get around," Krishnan said.

'THE LAST-MILE ISSUE'

One notable MaaS experiment is under way in Columbus, Ohio. There, Bytemark Inc., a New York City-based software-development firm specializing in transit, is working on a mobile wallet that will enable residents to plan, book, and pay for trips that include rides on Central Ohio Transit Authority buses, as well as bike and scooter sharing.

Bytemark is developing the app with MTech Solutions LLC, a Columbus-based geographic-information systems (GIS) software firm.

"It makes it much easier from a participant's view to address the

last-mile issue," says Eric Reese, Bytemark's president and chief executive and a former executive at the Chicago Transit Authority. "I have one source of funds to be able to pay for it. It is meeting the vision on what mobility as a service is."

The app is part of a multifaceted, $190-million areawide transportation improvement project called SMRT Columbus. Seed money came from a $40-million U.S. Department of Transportation grant Columbus won in 2016.

Riders already can use the so-called Pivot app for trip planning. Payment functionality is expected to go live in May, says Reese. The app produces a bar code on the rider's smart phone for presentment when boarding a bus, and also enables users to book Lyft rides as well as unlock scooters. Coming features include near-field communication technology for contactless transactions.

"We are in active discussions" with other cities about implementing similar solutions for their transit systems, Reese says. "It's something that is able to be replicated."

According to APTA's 2020 Public Transportation Fact Book, 36 transit agencies have mobility pilots going with Uber, Lyft, other private operators, or in-house operators. Denver's Regional Transportation District made news last year when Uber enabled riders to purchase RTD tickets through the Uber app.

'We're definitely headed in [MaaS's] direction.'

—**JEFF HIOTT**, VICE PRESIDENT OF TECHNICAL SERVICES AND INNOVATION, AMERICAN PUBLIC TRANSPORTATION ASSOCIATION

Earlier this year, Uber rolled out a similar service with the Regional Transportation Commission of Southern Nevada in Las Vegas. On both systems, payments are facilitated by transit-services software developer Masabi Inc.

APTA's Hiott says MaaS is making progress on the Dallas Area Rapid Transit system and at the Los Angeles County Metropolitan Transportation Authority, though full-blown MaaS has yet to be implemented.

'WE ARE STUDYING'

A private-sector strain of MaaS comes from Montreal-based Transit App Inc., which launched in 2012 with an app that enabled consumers to plan multi-modal journeys that integrated ride-share companies and, later, bike rentals. Today, Transit's iPhone and Android apps are integrated with various partners' application programming interfaces and tokenize the user's credit card for payment.

Behind the scenes, Transit creates accounts for the rider with each provider, but "from the user perspective it's just one thing," says David Block-Schachter, Transit's chief business officer. Block-Schachter formerly was chief technology officer at the Massachusetts Bay Transportation Authority in Boston.

The Transit app is now available in more than 200 cities worldwide, most of them in North America, including such big ones as New York, Washington, Los Angeles, Toronto, Montreal, and Vancouver.

Most of Transit's partners are private providers. Riders on only a few North American public systems can pay fares through the app. Participating systems include those in Denver, Las Vegas, Cincinnati, Santa Monica, Calif., and St. Catherines, Ontario.

"We'll be easily twice that by the end of the year," says Block-Schachter. "Our big push right now is on the public-agency side."

Still, MaaS remains a nascent concept for most transit executives.

"Like a true public agency, we are studying," quipped another Payments Summit panelist, Rhyan Schaub, director of fare revenue and administrative services at TriMet, the transit agency for the Portland, Ore., area.

One of TriMet's major recent accomplishments was creating a smart-phone-based virtual card for its Hop fare system. Some 25% of the system's active cards are now virtual, according to Schaub.

'Our big push right now is on the public-agency side.'

—**DAVID BLOCK-SCHACHTER**, CHIEF BUSINESS OFFICER, TRANSIT

'A LOT MORE PRACTICAL'

Indeed, replacing outmoded mag-stripe fare cards with chip-card-based contactless proprietary and open-loop systems and mobile wallets is a higher priority than MaaS at most agencies. APTA says 48% of transit systems offered smart card fare options in 2019, compared with only 12% in 2009.

By far the highest-profile contactless upgrade is going on in New York City, where the MTA eventually will have tap-and-go card and mobile-phone readers at all of its 472 subway stations, and on buses.

The system, dubbed OMNY and developed by Cubic Transportation Systems, enables riders to pay with major-brand contactless credit and debit cards as well as Apple Pay, Google Pay, Samsung Pay, and FitBit Pay.

OMNY also will have its own virtual card and a physical contactless card set to launch in 2021. The system is replacing the mag-stripe MetroCard, which debuted in 1994.

The MTA in December said it had surpassed 4 million taps since partial rollout began seven months earlier. Still, it's unclear whether riders will embrace open-loop contactless payments once the closed-loop card and virtual card are available.

At Portland's TriMet, open loop accounts for only 2% to 4% of payments. A pioneer in open-loop payments, the Salt Lake City-based Utah Transit Authority, which began tests in 2006, quietly dropped open-loop cards last year, saying they accounted for less than 1% of daily ridership.

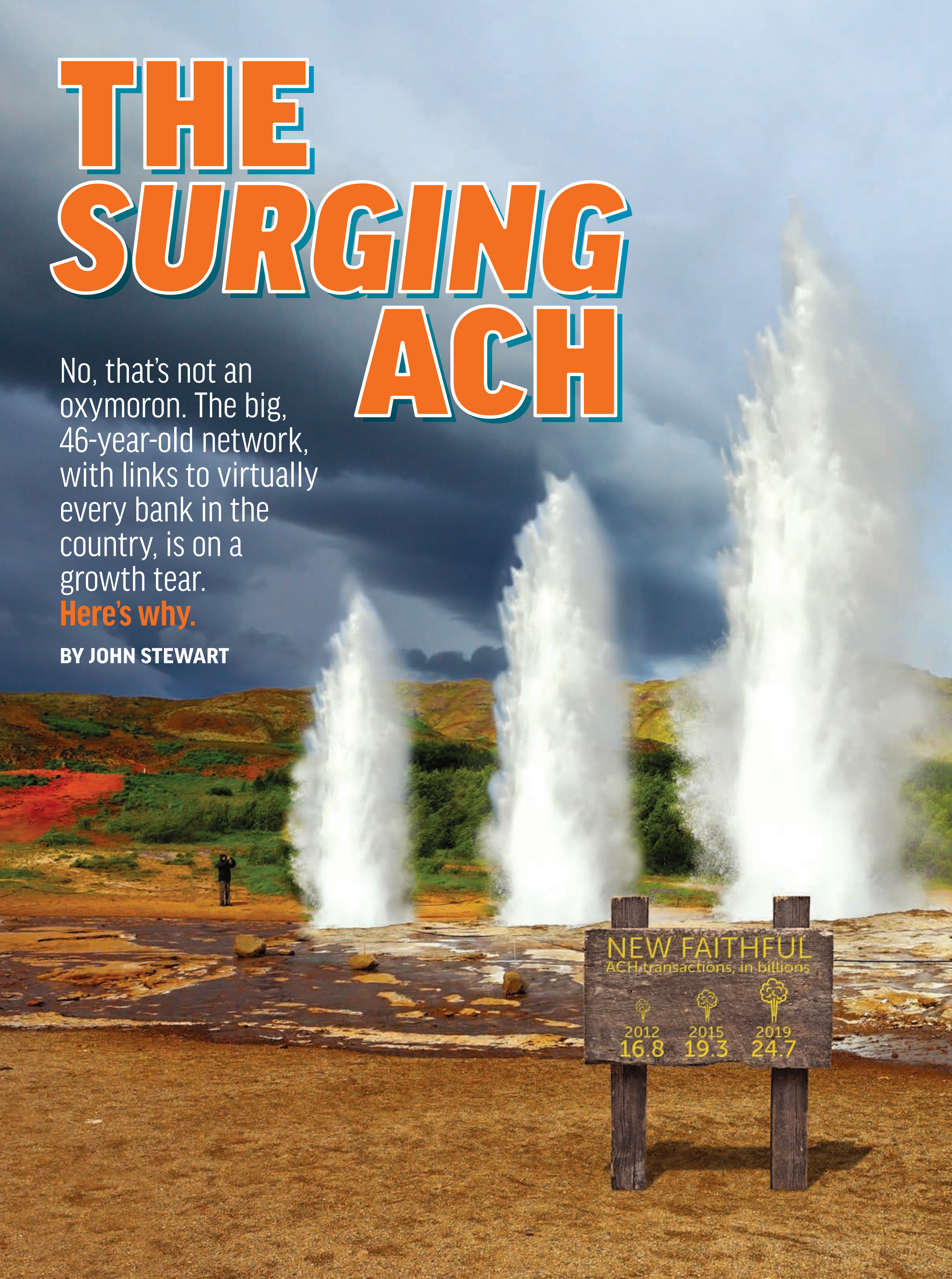
But the New York City area, which accounts for about 40% of the nation's entire transit ridership, has the heft to change the fortunes of open-loop contactless payments, especially now that banks and credit unions are pumping out contactless-enabled dual-interface EMV chip cards by the millions. Visa Inc. expects 300 million Visa-branded contactless cards to be in issue by year's end.

"It's a lot more practical … if it's not closed-loop," says Rachel Huber, senior analyst, payments, at Pleasanton, Calif.-based Javelin Strategy & Research. DT

THE SURGING ACH

No, that's not an oxymoron. The big, 46-year-old network, with links to virtually every bank in the country, is on a growth tear. **Here's why.**

BY JOHN STEWART



One of the biggest untold stories in the payments industry lies ready to hand for anyone who wants to check the numbers. It's about a network growing at a steady annual rate exceeding 7%.

At first glance, that may not seem remarkable. But the network is the automated clearing house, and with links to just about every financial institution in the country, it's huge. It's also old, founded in 1974, before the Internet, before mobile phones, and back when paper checks ruled supreme.

Big, sprawling networks with roots in old technology don't typically enjoy accelerating growth. But these days the stars are lining up for the ACH.

Today, checks are in decline, and the ACH is, relatively speaking, on a tear. Factors like the Web, the gig economy, slicker bill payments, and mobile person-to-person transfers are taking off, and what many don't see is that it's often the ACH operating the machinery behind the curtain.

'THE LEAST-COST PAYMENT'

That faster growth rate is also the result of an often overlooked economic fact. Compared to the card networks and even checks, the ACH is pretty cheap, something that just adds more momentum to the network's growth. "Cumulatively, it feeds on itself. It's the least-cost payment," says Bob Steen, chairman and chief executive of Bridge Community Bank in Mechanicsville, Iowa.

The network processed 24.7 billion transactions last year, up 7.4%. That follows an almost equally hot 2018, in which transactions grew 7%, adding impetus to a system that had been, relatively speaking, in the doldrums for years (chart, page 28).

"The statistics are showing an accelerating growth," says Michael Herd, senior vice president at Nacha, the Herndon, Va.-based organization that governs the ACH. In fact, he adds, "2019 was our highest growth rate since 2008."

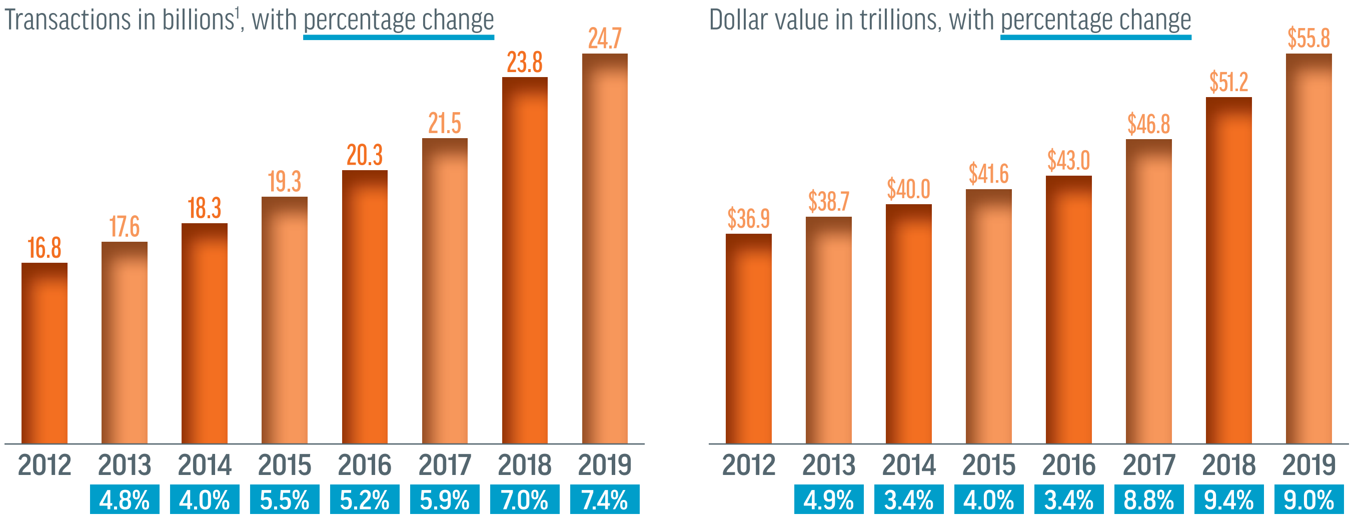
Processors that handle ACH transactions are reporting similar results. Growth lately "is really strong across the board," says David Fortney, an executive vice president at The Clearing House Payments Co., a New York City-based company controlled by many of the nation's biggest banks.

By "across the board," Fortney is referring to everything from business-to-business transactions moving away from checks to bill payments to peer-to-peer transfers.

Especially active in the B2B category, he says, are health-insurance remittances, which he says are finally moving away from checks. "It was a long time coming. I think we have several years of outsize growth potential there," he says.

All told, B2B transactions were up 12% last year, according to Nacha

THE ACH'S RAPID ASCENT



1. Network volume only. Excludes on-us activity. Source: Nacha

figures. Internet-based transactions are also on a fast-rising slope. These jumped 13% in 2019.

'REVENUE GENERATOR'

As some may ask, what took so long? Businesses are inherently conservative beasts, slow to adapt to new ways of doing things, including payments. Dealing with ACH files is no exception.

"It's just taken this long for everybody to get more comfortable," notes Michael Bilski, chief executive of Roseville, Minn.-based North American Banking Co. "It's just part of our vernacular now."

So much so that the economy, once swarming with checks, is seeing far fewer of the pieces of paper. Total check volume in 2018 came to 16 billion items, down 21% since 2015, according to the Federal Reserve's latest triennial payments study (chart, page 31).

Checks presented for payment, that is, not converted to ACH in biller lockboxes or at the point of sale, fell 18%. As a fraction of core non-cash payments, checks have dwindled from a 58.8% share in 2000 to 8.3% in 2018, the Fed data show.

"The shift in B2B payments from checks to ACH and other electronic transactions is happening," says Nacha's Herd. "There's been a prevailing conventional wisdom that businesses are stuck on checks. That's a myth."

Expert observers are seeing the same thing as lower costs and network reliability drive businesses to adopt ACH. "Banks and corporates are getting serious about embracing change," says Patricia Hewitt, principal at Savannah, Ga.-based payments consultancy PG Research & Advisory Services. "Banks are figuring out ACH can be a revenue generator for them, and corporates are getting more comfortable with it."

Or, as Bilski puts it: "ACH is really where it's at. It's cheaper and reliable as hell."

Where the switch away from checks is particularly apparent is in payroll, where businesses are increasingly seeking electronic methods to replace paper paychecks, Herd says. This effort involves a method called direct deposit, the original ACH application. "We're seeing a robust increase in use" of this channel, Herd notes. "Direct deposit is on fire."

He credits the shift to a trend exemplified by mobile-driven segments of the economy like ride-sharing platforms, which favor electronic deposit of payroll for its speed and practicality. Now, the ACH is looking at a related change that could meet operators' requests to be able to pay gig workers more often.

"We're hearing what industries are interested in is more frequent payment cycles, not just faster payments," Herd says. "We have the capability of supporting more-frequent paydays. We are listening and responding."

'PATH OF LEAST RESISTANCE'

Another recent change in payments technology is also fueling ACH growth. That 13% rise in Internet

A CREDENTIAL CHECKER FOR THE ACH

A platform to help ensure payments are made to the proper entity is set to debut next month. Dubbed Phixius, the Nacha-developed platform will provide a way to enable the secure sharing of payment-related information.

That's important because the platform, announced in February, could save businesses time in vetting new payees and ensuring the payment is properly made, Nacha says.

Phixius will not be a conduit for payments. Instead, Phixius supports payment information shared between payees and payers and can include instructions for multiple payment types, including ACH, wire, card, and others, says George Throckmorton, Nacha managing director and executive director of Afinis Interoperability Standards. "It's within the instructions that the payment type is specified," he says.

Afinis is a standards organization under the auspices of Herndon, Va.-based Nacha, the rules-setting organization for the ACH.

Phixius, which the consulting firm Ernst & Young LLP helped develop, will be the enabler for credential-service providers and will authenticate their customers and establish trusted information about them, such as mailing address and telephone number, Throckmorton says. Credential-service providers will provide downstream services to the business, which likely won't even be aware of Phixius, he says.

In one possible use case, an employee in an accounts-payable department needs to issue a check to a new vendor, but the vendor must be added to the company's master list of accounts. As things stand now, Throckmorton says, that process can be time-consuming. Typically, businesses have approximately 3,000 accounts on the master list, he says.

To enroll the vendor, the employee has to find the relevant data. That's where a credential-service provider connected to Phixius can expedite the process, Throckmorton says. "They can strongly authenticate with their customers," he says of the credential-service providers. They then, within moments, can share that trusted information with their client so a payment can be issued. It automates a task that currently is a manual one, Throckmorton says.

And if the provider does not have the vendor's trusted information, it can connect to Phixius and check if another Phixius provider might have the information, he says.

The two roles for Phixius are to enable the sharing of this trusted information and to ensure the information is up to date, says Throckmorton.

It will accomplish the latter by sending notifications to credential-service providers whenever the trusted information for a participant is updated, Throckmorton says. That will be made possible by using blockchain technology.

Phixius also will incorporate application programming interface technology and rely on its Afinis Interoperability Standards to help ensure the system works across users.

There will be a fee to connect and use Phixius, but when last checked this was still being determined.

—Kevin Woodward

payments last year had much to do with consumers funding digital wallets from a growing variety of fintech companies.

Meanwhile, fintechs like Plaid Inc., which Visa Inc. in January agreed to buy for $5.3 billion, act as "enablers" of the ACH's rising volume of digital payments, according to Herd.

Plaid, founded just seven years ago, connects payments start-ups with their customers' bank accounts. That funding access is what San Francisco-based Plaid enables for a range of companies, many of which didn't exist a decade ago, including fintechs like Acorn, Betterment, Chime, and Square, as well as Stripe and Venmo, a unit of PayPal Holdings Inc.

But ACH payments rely on information that may not always be practical to obtain, such as a recipient's account number and bank routing number.

"There are multiple directories that help to do that, but they aren't necessarily complete," says Sarah Grotta, director of the debit and alternative products advisory service for Mercator Advisory Group, a Marlborough, Mass.-based consultancy. "Clarifying that area is a good place to start."

One solution aiming for that clarification is a Nacha initiative called Phixius, set to start up next month to act as a directory for ACH payments (box). Without some kind of easily accessed, accurate information, many businesses are likely to go on writing checks, say some observers. "A business will write a check because it's the path of least resistance," Grotta says.

Even now, though, there are signs that may be changing. "We're seeing more and more invoices with the ACH information with them," says Steen of Bridge Community Bank. He notes this is a big change in just the past two years.

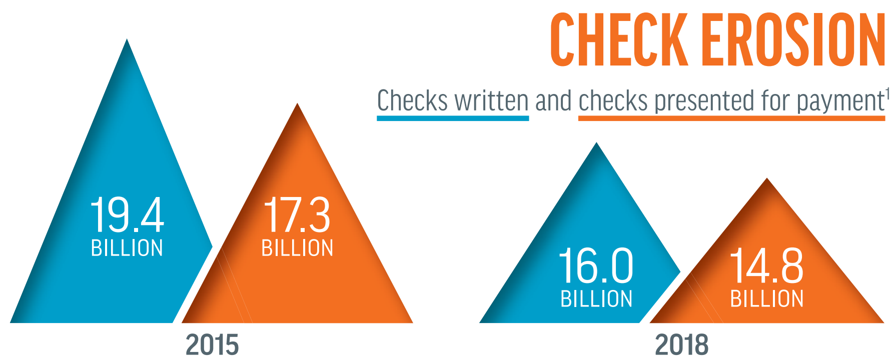
'PLEASANTLY SURPRISED'

For now, the ACH is gearing up for future growth by addressing the demand from business for faster payments. Nacha introduced same-day credits in 2016 and then debits a year later, and by all indications the new categories are taking off fast.

Same-day payments, which shave a day off the typical two-day processing-and-settlement time for ACH, totaled 250.4 million in 2019, up 41% from 2018. Dollar value came to $247 billion, a 55% annual increase. That comes to just 1% of all ACH transactions, but businesses are watching that number closely as they respond to increasing pressure for faster transactions.

Faster payments are especially critical in the newer transaction categories like ride share and free-lance services, which are adopting the option. "Same-day ACH is growing very quickly," says TCH's Fortney, whose company offers a fledgling real-time payment service to help slake the growing thirst for faster payments. The same-day numbers posted in 2019, he adds, represented "a big milestone."

Even faster growth could be on the horizon. Nacha last month implemented a rule raising what had been a $25,000 ceiling on same-day transactions to $100,000. And in March next year, the network is set to add a third settlement window at the end of the processing day.



1. Not converted to ACH. Source: Federal Reserve Payments Study

Under the rule change, the Fed will keep its National Settlement Service open until 6:30 p.m. Eastern Time, one hour later than its current closing time. The Fedwire Funds Service will stay open a half hour longer until 7 p.m. As a result, the latest daily deadline for same-day ACH will occur at 4:45 p.m. Eastern Time, two hours later than the current cut-off.

That move is expected to open a geyser of volume from the Western states, which will get more time to submit transactions each day. Even now, some 4.5% of all new volume on the ACH is processing as same-day transactions, according to Herd. "We have been pleasantly surprised," he says, by the uptake of the service so far.

'A WHOLE NEW CHANNEL'

One other source of potential volume lies in selling merchants on using debit cards that rely on the ACH rather than the card networks. Some companies active in this area see potential in convenience stores and gas stations, which face a daunting task getting ready for a card-network deadline later this year to convert to EMV at their gas pumps.

Companies that aren't ready for EMV will bear responsibility for card fraud. "The petroleum and convenience-store industry are going to get shocked by the liability shift," says Mark Horwedel, a payments-industry consultant. "It will be interesting to see what they do with all the fraud coming their way."

Sensing an opportunity, Buy It Mobility Networks Inc. offers a mobile app consumers can use to pay merchants directly from their bank account. "We're opening up a whole new channel for ACH," says Adam Frisch, the company's founder and chief executive.

BIM, which has deals with some major brands, including Shell and Phillips 66, stresses consumer rewards, such as discounts off each gallon of gas, to boost adoption and usage. Merchants pay for the rewards, but feel they are still ahead of the costs of credit card acceptance, Frisch says.

Much the same logic could apply in other merchant categories, even without the costs and pressure of an EMV conversion. If that proves true, the ACH could be entering a golden age, particularly if consumers respond favorably. Few of them, however, are likely to mind how their transactions are processed.

As Steen of Bridge Community Bank says, "Consumers don't care about the plumbing." DT

LOCKING DOWN APIs

Protecting the ubiquitous code that enables untold numbers of payments connections is no easy matter. It's also critical.

BY **KEVIN WOODWARD**

JUST HOW ATTRACTIVE to criminals are the networking connections between payments and financial-services companies, on the one hand, and third parties, on the other? Extremely.

Witness that one day in August 2019, a single financial firm weathered more than 55 million malicious login attempts by criminals trying to stuff their collection of ill-gotten personal information in the firm's Web pages.

The bad guys, in this instance, were not successful, says the security company Akamai Technologies in its "State of the Internet/ Security" report released earlier this year, which cataloged the attack.

What are application programming interfaces (APIs) and why are they so important? They enable sharing information without cumbersome logins. They're the software code, for example, that enables a third-party to move funds to your bank account. Just as important, they segregate information to make it tougher for criminals to access it.

APIs have been active for some time in some very prominent payments programs. They make it possible for Green Dot Corp., for example, to enable Apple Inc. to link Apple Pay to Green Dot's infrastructure. "While regulatory issues still need to be managed by Green Dot, the technical connectivity to the Green Dot infrastructure becomes simple," says Tim Sloane, vice president of payments innovation at Marlborough, Mass.-based Mercator Advisory Group Inc.

"APIs enable companies with no experience in payments to quickly integrate their systems and software to payment experts and rapidly start transacting payments," Sloane continues.

Further, APIs make banking programmable, says Ron Van Wezel, senior analyst at Aite Group LLC, a Boston-based consultancy, "allowing third-party developers


ONLY ONE OF THESE BIRDS CAN
GIVE YOU THE LATEST NEWS
IMPACTING THE PAYMENTS MARKET
Today and every day follow
DIGITAL TRANSACTIONS
@DTPAYMENTNEWS on Twitter
DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

(fintechs and others), to access bank data and functionality to create new value for customers."

This has led to open banking on a global scale, he says, and holds still greater promise. "While still in initial stages," he adds, "open banking will lead to the next wave of digitization in payments, reconfiguring age-old value chains and changing business models."

'TIME-BASED ROI'

Adapting existing models to the capabilities afforded by APIs, and the creation of new ones, won't happen smoothly unless these connections are protected. Protecting APIs is vital because criminals have incorporated them into their target portfolios.

Criminals want to access data held by financial-services companies because that's where the money is. But this data also includes personal information associated with a victim's financial account, says Steve Ragan, an Akamai security researcher. "Information has value, and can be sold or traded," Ragan says.

'Think about the other businesses you are making APIs available to or using APIs from, and question their security practices.'

—**KEITH FULTON**, SENIOR VICE PRESIDENT AND CHIEF INFORMATION OFFICER OF BANK SOLUTIONS, FISERV INC.

"When criminals are targeting APIs, they're attempting to bypass defenses and target as many accounts as possible," Ragan says. "[Multifactor authentication] makes things harder for the criminals, not impossible, but certainly harder."

Online criminals follow patterns similar to those they observe in the physical world. The time needed to commit the crime, for example, should not outweigh the perceived return on investment.

"There is a time-based ROI for a lot of criminals," Ragan says. "If an account doesn't fall instantly to a username/password combo, they move on to a new account. Only the more dedicated ones will attempt password variations or move on to phishing in order to attempt a multifactor authentication bypass."

APIs are subject to a number of common threats, says Johannes Ullrich, dean of research at SANS Technology Institute, a cooperative research and education organization. "Encryption, since [APIs] go over public networks, is a problem," Ullrich says. "They have to know who is sending the request. Then ensure the message is not altered as it's transmitted."

Protecting the integrity of API connections also buttresses any service guarantees ensuring a certain number of API connections for authorized users, he says.

Generally, API protection starts with the concept of least privilege, followed by fail-safe defaults (meaning a user's access should be denied unless granted access explicitly), Ragan says.

Multiple security considerations come into play, says Mathieu Auger-Perreault, director of fraud and security at Pleasanton, Calif.-based Javelin Strategy & Research.

"Securing APIs, just like securing other components of the payments ecosystem, requires multiple layers of defense, including making sure API developers are aware of security risks and best practices," Auger-Perreault says in an email.

Among Auger-Perreault's considerations:

- Is the communication channel secured?
- What kind of data is the API providing? Is it providing too much information versus what is required?
- How are API requests authenticated and authorized?
- Is the API vulnerable to injection attacks?
- Is the API producing logs and are these logs collected and analyzed by the security team?

Actions and techniques to answer these questions include involving the organization's technology security team in API development, Auger-Perreault says. Others are to use encryption and adopt a need-to-know or least-privilege mindset when deploying APIs that also include the data these APIs provide.

API managers should keep several factors in mind, says Keith Fulton, senior vice president and chief information officer of bank solutions at Fiserv Inc. "Business owners should think about the level of security they need–where does the use case fall on a security spectrum?," Fulton says

NORTH AMERICAN BANCARD FUELS GROWTH FOR SALES PARTNERS AND ISOs

Business today is complicated as consumer needs and expectations shift. Whether it is about speed or the customer experience, more is expected, at an unprecedented pace. Merchants looking to manage consumer expectations in the payments arena often need help from a payments expert (sales partner) that is intune with the shifting market needs. Sales partners offer a unique consultative approach merchants need to help them respond to the shifting landscape.

For more than 25 years, North American Bancard has worked hand-in-hand with sales partners and ISOs to help them compete, and win, in the merchant marketplace. As business has evolved, so has NAB's support and dedication to its partner program.

Furthermore, as the payments industry continues to consolidate and companies are concentrating more effort on creating synergy versus boosting sales partner programs, NAB remains committed to investing in its salesforce.

Here's a look at the latest program features NAB has introduced.

REFRESHED PEAK BONUS PROGRAM

We've been busy at NAB in the new year as we work hard to structure and retool programs for our partners. One exciting initiative is the revamped PEAK bonus program. The revised program offers greater incentives in the form of a $500 upfront activation bonus, an increased multiplier of 14x, and a doubled cap to $10,000 per merchant to sales partners who sell the Payanywhere Smart Solutions to merchants boarded on Electronic Payment Exchange (EPX), NAB's wholly-owned payment processing platform.

This program helps sales partners get modernized payment solutions into the hands of merchants, while also enhancing portfolio profits.

40X RESIDUAL BUYOUT OFFER

The newest NAB buyout offer puts a new spin on the program. The incentive gives sales partners the option to have 50 percent of their portfolio purchased at 40x, giving the partner a larger cash base to invest in business enhancements and/or hire new field representatives. This option is even available for portfolios not with NAB today! It's truly a win-win for savvy sales partners with growth in mind.

The newly structured program is available to both existing and new sales partners with NAB.

TRANSCEND: THE PREMIERE PARTNER EVENT

NAB's flagship partner event is hitting its third year and promises to be another can't-miss event. Partners, attendees, and sponsors are treated to an unforgettable experience featuring new product announcements, educational seminars on the future of payments and how to sell effectively, and valuable networking sessions tailored to growing portfolios.

Transcend includes sessions on simplified selling solutions, such as NAB's POS Pros, a program designed to help sales partners close more deals via dedicated staff who work to customize programs that fit the unique needs of each merchant.

Past Transcend events have included keynote speakers such as Chris Gardner, Ryan Estis, Molly Bloom, and Jordan Belfort, who've all shared insights on winning in competitive situations. Transcend is where payment innovations meet real-world implementation.

Sales Partners have the knowledge base and consultative approach merchants need to compete in business today. North American Bancard realizes how valuable sales partners are and will continue to develop new and innovative programs, educational resources, and modern tools to help them grow. If you're interested in joining NAB as a sales partner, please visit www.gonab.com or call 877-812-8041 to learn more!

NorthAmerican® BANCARD

by email. "Any API that involves the transfer of personally identifiable information, or the movement of money, must be secure.

"Think about the other businesses you are making APIs available to or using APIs from, and question their security practices," Fulton continues. "This is a situation where the chain is only as strong as the weakest link. If the businesses you connect to are not practicing good security habits, that can put your business at risk as well."

'Traditionally, encryption and some sort of authentication formed the bulk of API protection efforts, but those steps alone are no longer sufficient.'

—**SAM PFANSTIEL**, DIRECTOR OF SECURITY CONSULTING SERVICES, CONTROLSCAN INC.

BEHIND THE ENDPOINT

Traditionally, encryption and some sort of authentication formed the bulk of API protection efforts, but those steps alone are no longer sufficient, says Sam Pfanstiel, director of security consulting services at ControlScan Inc., an Atlanta-based data-security provider.

Today, securing an API entails peeling back to what's behind the endpoint—that's technical speak for the very end of the connection enabled by the API—Pfanstiel says.

"Is the software being developed by a programmer trained in software security?" is one of the questions to ask. Does the software code have some sort of separation of duties, so if one component is compromised it's less likely to spread? Today, protection APIs involve encryption, authentication, security development, empirical testing, and separation of duties, Pfanstiel says.

Mercator's Sloane advocates a sandbox approach. That segregates the API and its specific task so it can be tested in as close to a real-world environment as possible.

"Then a proactive vetting of the user organization by the payment platform and bank to validate the use case, the adherence to regulations, and the availability of funds," Sloane says.

"With all of that in place," he continues, "the only thing left to do is to have a development team that follows traditional banking-system development and personnel management policies to prevent against insider attacks, blackmail, trap doors, etc."

APIs can be written in any computing language and sometimes can be so numerous an organization might lose track of all the APIs it allows, says Ullrich. "The API represents your business logic," he says. "They can all implement their own front end. The value is providing the standardized interface."

Payments and financial-services entities are working on API standardization, too. Nacha, the Herndon, Va.-based automated clearing house governing body, created the Afinis Interoperability Standards body to advance API standardization.

And nonprofit Financial Data Exchange has an overall mission of fostering common, interoperable standards for access to financial data. It is an independent unit of the Financial Services Information Sharing and Analysis Center, a Reston, Va.-based association.

MOVING MONEY

Using best practices to secure APIs will only become more important as the use of APIs proliferates. "The speed with which businesses can adopt new payment strategies and innovate will continue to increase significantly," Sloane says. A new range of use cases, potentially disruptive ones, will start to appear, he says.

"In some instances, these will be implemented by innovations in a siloed payments infrastructure, while in other cases it may be implemented on top of a regulated standard as may become possible under the PSD2 standards across all [European Union] banks," Sloane says.

"These payment APIs," he continues, "could in essence allow new payment schemes that totally bypass the traditional payment networks. In short, APIs will continue to speed up disruption."

Auger-Perreault has a similar take. "APIs will enable 'fast followers' in the payments space to keep pace with more powerful and well-funded financial brands ratcheting up the competitive landscape," he says. "APIs are critical to the infrastructure of payments and enable money to move." DT

SPONSORED CONTENT

MERCHANTS TURNING TO SMALL BUSINESS CREDIT CARDS TO IMPROVE CASH FLOW

ISOs tap into card issuing revenue

One of the biggest challenges for small businesses is the availability of credit according to a recent study[1] by the Federal Reserve.

Many merchants address this by taking out short-term business loans or using personal credit cards to bridge the gap. While credit cards with a revolving line of credit are a good funding source for merchants, many do not qualify for the ridged underwriting policies of most, if not all, the major banks.

While using personal credit cards to make everyday business expenditures solves the short-term problem, these cards can take a toll on the business owner's personal credit score which will further inhibit the business owner to finance their personal needs, such as refinancing their home or purchasing a car.

PAYVUS: THE SMALL BUSINESS CREDIT CARD PROGRAM BUILT FOR ISOs AND ACQUIRERS

Historically, banks decline the vast majority of small business credit card applications because it is very difficult for the banks to assess the risk of newly opened businesses, sole proprietors or business owners with low credit scores. Merchant's daily card processing receivables are rarely taken into account by banks when assessing risk. The missed opportunity for these banks is a new opportunity for ISOs and Acquirers.

Aliaswire has designed a small business credit card specifically built for the types of merchants served by merchant service providers. By leveraging the merchant's card processing receivables, the PayVus® credit card enables merchants to take control of their cash flow and gain access to a small business credit card.

With PayVus, your merchant will be issued MasterCard World Elite Business Credit Card with a line of credit based on their FICO score – up to $10,000. The PayVus technology platform split-settles a portion of the merchant's daily card processing deposits to the PayVus credit card. The combination of the PayVus card's line of credit combined with the daily deposits to the PayVus card provides greater purchasing power for the merchant and helps the merchant better manage cash flow.

Aliaswire provides a revenue share to the ISO/Acquirer from interchange generated when merchants make purchases with the card. ISOs and Acquirers can use the revenue share to reduce merchant processing fees. This new approach to merchant acquiring can yield significant savings through the reduction of merchant processing fees.

For the merchant, the PayVus card provides a revolving line of credit to the business without a personal guarantee and, unlike debit cards, the transacting on the PayVus card helps the merchant build a credit history. Additionally, traditional card reward programs have limits on rewards whereas PayVus has no limit on savings.

A NEW REVENUE SOURCE FOR MERCHANT SERVICE PROVIDERS

Aliaswire provides a revenue share to the ISO/Acquirer from interchange generated when merchants make purchases with the card. ISOs and Acquirers can use the revenue share to reduce merchant processing fees. This new approach to merchant acquiring can yield significant savings through the reduction of merchant processing fees.
For the merchant, the PayVus card provides a revolving line of credit to the business and, unlike debit cards, the PayVus card helps the merchant build a credit history.

Every business makes purchases, for supplies, inventory, software or meals. ISOs and Acquirers can – and should – capitalize on this opportunity by providing their merchant with a credit card for making purchases and managing business expenses. Providing merchants an integrated AR/AP solution, paves the way for stronger and longer-lasting relationships, reducing churn and increasing ISO/Acquirer revenues.

1. 2019 Report on Employer Firms – Federal Reserve Bank

One-dimensional fraud solutions are inadequate for today's complex environment.

endpoint

THE FUTURE OF E-COMMERCE

The best place to start fighting fraud is at the first interaction, not at the order form.

BY **BRAD WISKIRCHEN**

Brad Wiskirchen is chief executive of Kount Inc., Boise, Idaho.

MORE AND MORE BUSINESSES are seeing the convergence of fraud prevention, cybersecurity, and customer experience. From preventing the theft of data to stopping chargebacks to protecting the customer journey, there is a need to balance these three areas and work cross-functionally to achieve business goals.

What have been traditionally cyber events alone now lead to fraud, including events such as ransomware, business email compromise, identity theft, synthetic ID, and stolen credentials. At the center of this cycle is account takeover, fraudulent accounts, and payments fraud. And that means modern fraud risk is changing.

No longer is risk solely focused on chargebacks. It now encompasses regulatory concerns, poor conversion rates, brand reputation risk, data security, credit, poor customer retention, and more.

As digital innovation continues to scale and customers expect less friction as they complete checkouts, businesses must take a multifaceted approach to fraud prevention that spans the entire customer journey.

IDENTITY TRUST

In a recent survey conducted by Kount and Javelin Research, 42% of businesses reported that digital fraud slows their ability to innovate and expand into new digital channels and services. At the same time, only 64% of customers have confidence in the security of digital channels. And 48% of customers are more sensitive to anti-fraud measures that disrupt their online experience than they were a year ago.

Compounding these trends, businesses reported that top fraud threats include payments fraud, account takeover, fraudulent accounts, and friendly fraud.

With the need to balance fraud, cybersecurity, and customer experience along with ever-evolving emerging fraud types, it is increasingly critical that fraud prevention not overly rely on any one tactic. Solutions that are one-dimensional cannot solve the complex business needs of today's digital risk management.

Effective fraud prevention must get to the core of identity trust. Identity trust is the ability to establish the level of trust for each identity behind every payment, account creation, and login event.

Think of it as a spectrum: on one end is the lowest trust level, likely indicating fraudulent activity. These interactions should be blocked or encounter high friction. On the opposite end of the spectrum is the highest trust level, which includes returning, quality

STRAIGHT TALK FOR ISOs

A Q&A from First American's Angela Carranza and Ross Paup

"Relationship" has become a dirty word in the industry. It's overused and empty. What's so different about the First American approach?

Angela: We take the time to know our prospects from both a business and personal level. We also invite potential partners to our corporate office to meet everyone—the CEO, the underwriters, customer service reps, product and integration teams, and marketing. How many CEOs do you know who will actually take the time to get to know a prospect? How many companies do you know that encourage partners to call when they need help solving a problem or simply want to tap into a team's expertise? Once a prospect becomes part of the First American family, we collaborate with them to add value to their brand, whether that's through integrations, products or marketing.

Are last year's mergers really the big bad boogey man? How is First American faring?

Ross: The acquisition activity has, in most cases, had a negative impact on the level of service and support the ISOs working with those companies receive. While many of the acquired companies are justifiably focused on merging systems, platforms, and products, our focus continues to be on helping our ISOs grow and evolve in the market. As a privately held entity, First American is nimble, offering a true one-to-one partnership with our ISOs, a benefit which has only become more important during all of the M&A activity during the past 24-36 months.

ISOs are exhausted by unmet product promises. How is First American's product strategy energizing ISOs and helping to distinguish them in the market?

Ross: Many companies will develop a solution they believe in and then hope their customers fall in line to sell it. First American tailors and builds solutions to meet the needs of the merchant and the opportunities in the market.

Angela Carranza is Manager, Strategic Partnerships

Ross Paup is Senior Manager, Strategic Partnerships

This partner-centric approach is not always the easiest path, but it continues to generate success among our ISO partners and ensures a better merchant experience.

Put real dollars and a real-life use case to how your company has legitimately helped an ISO accomplish its growth targets.

Ross: Our willingness to adapt to the need at hand is the key. In many cases, tailoring a solution has nothing to do with the payment processing or software, it may be as simple as boarding, underwriting, or other operational efficiencies. One of our ISOs, for example, wanted to provide a custom, simplified merchant experience for a marketing organization with a large number of retailers. We created a custom pricing model, boarding process, and payments integration to work within the ISO's mobile application. As a result of First American's custom underwriting and onboarding solution, nearly 80,000 retailers migrated to the new system within the first 60 days.

In one sentence, tell the ISOs reading this piece why First American is worth their time.

Angela: First American creates tangible value for our partners through high-touch relationships, custom integrations, product solutions and award-winning support.

customers. These customers should not only be allowed through, but also treated like VIPs. That's one way identity trust bridges fraud prevention and customer experience.

Further, cybersecurity comes into play when considering that fraud prevention must span the payment transaction through the customer journey. From the moment a customer visits a Web site, to account creation, to login, to a payment transaction, there is opportunity to establish identity trust.

Most companies engaged in e-commerce are aware of and working with solutions like Kount to prevent payments fraud. Yet, many aren't as well-versed in account takeover, and they should be.

A LAYERED APPROACH

To effectively prevent account-takeover fraud, businesses should look at three key layers in an ATO solution: protection, policy and customization, and reporting and data presentation.

At the protection layer, solutions should evaluate user behavior, device and network anomalies to detect high-risk, anomalous login activity such as bots, credential stuffing, and brute-force attacks. This helps determine in real time whether a login should be allowed, declined, or challenged with step-up authentication.

In the policy and customization layer, customers should be able to customize user experiences and reduce friction by identifying and segmenting users based on common characteristics, such as VIP users or trial users. A rich set of data is essential for delivering adaptive friction with the necessary precision. This dataset includes user type, device specifics, IP risk, geolocation, custom data, and more.

Some users are higher risk, some users are no-risk, and some users might require a personalized experience. Creating policies based on robust data allows businesses to decide what type of experience to deliver to their customer, from low friction to step-up authentication.

The reporting and data layer should provide login trend data that includes device and IP information, both of which are often not available to fraud teams. Having the ability to quickly identify and report on failed login attempts, risky IPs, compromised accounts, and inbound anomalies not only allows businesses to stop account-takeover attempts, it uncovers trends that enrich their own data and inform future policies.

With this layered approach, companies have access to a unified and customizable solution to combat malicious logins and bots, credential stuffing, and brute-force attacks while also enabling personalized customer experiences through an adaptive-friction model.

Fighting fraud is a multifaceted endeavor, and the best place to begin is at the very first interaction, not at the order form. That takes coordination across teams, organizations, and processes, and it's also the future of fraud prevention.

IT'S TIME TO STAY SAFE

Keep your client base and your income secure:

- *NLS offers flexible, customizable programs that don't just finance bankcard equipment, but also small business equipment and signs. New, old and refurbished.*
- *Score your own leases any time, from anywhere, on our portal.*
- *ZERO month recourse*
- *Enjoy generous cash bonuses for volume and commitment*
- *Earn top dollars for referrals*
- *PLUS the best factors in the industry!*

There is no better time to give your clients a competitive edge. And give your business the stability it needs.

Reach out to NLS Equipment Leasing today:

NLS
EQUIPMENT FINANCE LLC

Deepika Shahani
877.245.4686
Deepika.Shahani@nlsequipment.com

www.nlsequipment.com

We've got a lot of bright ideas when it comes to growing your portfolio.

Partner with

HUMBOLDT

Partner with Humboldt Merchant Services to start powering your portfolio with retail, ecommerce, and specialty merchants. Our Sales Partner Portal allows you to effortlessly review merchant processing and residual data wherever, whenever. That means we've made it easier than ever to stay on top of your portfolio while allowing your merchants to take advantage of:

Specialized chargeback reporting.

Multi-currency conversion.

A full suite of anti-fraud services.

A boutique client experience.

Make the switch. Join the 25-year industry leader today.

855.767.0685 | HBMS.COM

Industries we specialize in:

Adult Content · Bail Bond Issuers · Business Opportunity · Buying Clubs · CNP Tobacco · Dating
Direct Marketing · E-Cigarettes · Firearms & Ammunition and many more

Since 1992.