DIGITAL TRANSACTIONS®

Trends in the Electronic Exchange of Value

13TH ANNUAL

THE 10 MOST PRESSING ISSUES IN E-PAYMENTS

Volume Sixteen, Number Eleven • DigitalTransactions.net • November 2019

ALSO IN THIS ISSUE:

Fiserv's First Data Rationale

Risks And Rewards in CBD

Don't Get Caught in Europe's Net

Tap & Pay's Transit Magic

Pay-at-the-table is here.
And it's FREE!*

SkyTab™ is the game-changer you've been waiting for. You can now offer a cutting-edge pay-at-the-table solution to your merchants for FREE! SkyTab is fully integrated with all Harbortouch systems so servers can seamlessly accept payment directly from the table. But SkyTab offers much more than just payments...

- Pay-at-the-table including ability to add tips and split checks
- Re-order items directly from the table (full ordering functionality coming soon)
- Accept EMV, NFC and swiped card payments
- Built-in customer satisfaction surveys with manager alerts for low ratings
- Ability to collect customer emails to build a marketing database
- Integrated receipt printer and e-receipt functionality

Contact us today to supercharge your sales with SkyTab!

Rich Lopez, National Sales Manager East - 800-201-0461 x 1205 or rlopez@harbortouch.com
Max Sinovoi, National Sales Manager West - 800-201-0461 x 1219 or msinovoi@harbortouch.com
or visit www.isoprogram.com

HARBORTOUCH®
A SHIFT4 COMPANY

*Free equipment program requires Merchant Processing Agreement. Terms & Conditions apply.

S3584_08182019

contents

NOVEMBER 2019 • VOLUME 16, NUMBER 11

13TH ANNUAL

The 10 Most Pressing Issues in E-Payments 16

What's keeping you up at night? If you said nothing, you're lucky.
Here's a list of the biggest issues troubling most payments executives today.

THE GIMLET EYE The P2P Trap 4

TRENDS & TACTICS 6

How First Data Cemented Fiserv's Payments Strategy

A top Fiserv executive says the deal had much to do with the firm's big need for a merchant acquirer.

An ISO's $135-Million Win Against Global Payments

Looking for a David Beats Goliath story? Have we got one here.

Samsung Pay Makes Its Move(s)

Long quiet, Samsung's mobile-payments app is going after cross-border payments and offering a virtual prepaid card.

Payments Dominate Fintech M&A

Don't look now, but the payments category accounts for some of the biggest M&A deals this year.

Plus, Security Notes paints a sobering picture of what artificial intelligence can do in the wrong hands.

ACQUIRING 12

The ABCs of CBD

Some ISOs are high on selling acceptance services to marketers of this hemp derivative. The profit potential could be big, but so are the complications.

STRATEGIES 24

Europe's All-Embracing Data Regulations

Payments companies that handle consumer data in Europe are becoming quite familiar with the General Data Protection Regulation and the Secure Customer Authentication rules. Think you're immune because you're a U.S. company? Think again.

COMPONENTS 27

Tap-And-Pay's Express Train

After years of looking to make fare payment easier, mass-transit agencies have found the answer in contactless cards. That's giving consumers a compelling reason to use contactless on a broader scale.

ENDPOINT 31

Fraud Control: Good News, Bad News

On the one hand, fraud losses continue a seemingly inexorable rise. On the other, there are positive steps businesses can take to mitigate those losses.

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.

the gimlet eye

THE P2P TRAP

WHEN THE NEWS BROKE A FEW WEEKS AGO that PayPal is planning to attach a credit card to its Venmo peer-to-peer payment service, it didn't surprise many in the payments industry. In fact, the only surprise may be why this move took so long.

For years, PayPal has been looking for ways to wring revenue out of its fabulously successful P2P service. As with Zelle, Venmo's big bank-owned rival, payments on Venmo are free to users. So the irony is that the more successful Venmo is (at least in terms of usage), the bigger the drag it poses to PayPal's bottom line.

Venmo has unquestionably been a success. The service is just 10 years old. It was snapped up in 2012 for $26.2 million by a Chicago-based processor called Braintree, which in turn was acquired in 2013 by PayPal for a whopping $800 million. That deal was arranged by PayPal's then-president David Marcus in his pre-Libra days. In April, PayPal revealed Venmo had attracted more than 40 million active users. In July, it said these users had generated $24 billion in volume in the second quarter, up 70% year-over-year.

That's a lot of money—and a lot of free usage that PayPal increasingly can't afford. Quarter after quarter, PayPal reports that Venmo has been partly responsible for driving down its parent's take rate—the portion of each transaction it keeps, and a number closely watched by Wall Street.

PayPal hasn't been idle in this matter. Without charging for Venmo payments, it has introduced a range of fee-bearing services based on Venmo, including instant withdrawals, payments at merchants, and a Venmo-branded Mastercard debit card. In October came the latest gambit. PayPal announced it would launch a Venmo credit card issued by Synchrony Financial, which potentially could generate a lot more interchange revenue than the debit card.

Zelle, which is owned by Early Warning Services LLC, a company in turn set up by seven major U.S. banks, is in much the same position, having generated $44 billion in transactions in the second quarter.

So, what to do? PayPal's answer has been to keep tacking on related services it thinks users—or merchants—will pay for. Hence the instant withdrawals and that latest move, the credit card and the hoped-for interest income and interchange.

Why, you may ask, don't these P2P services just charge their users? After all, if the transfers are so popular, surely users will pay at least a modest fee? That's a good question, and one we haven't heard an answer to yet. Here's our take. Companies like reporting big numbers. The fear may be that P2P is wildly popular only so long as it's free.

John Stewart, Editor | john@digitaltransactions.net

NOVEMBER 2019 • VOL. 16, NO. 11

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.

NLS Equipment is a new leasing company totally committed to helping ISOs profit from microticket leasing.

- Flexible programs from $500 – $10,000
- **ZERO payment recourse** programs for qualified ISOs
- Direct lender: no middleman

WIN A CRUISE!

Fund more than ten deals before 2020
and we'll send you sailing.*

Take another look at leasing by contacting:
Deepika Shahani
Deepika.Shahani@nlsequipment.com
877-245-4686
nlsequipment.com

NLS
EQUIPMENT FINANCE LLC

New Company. Better than ever leasing programs.

* Deals must be funded before 2020 and are limited to programs with standard lease rate factors.

HOW FIRST DATA CEMENTED FISERV'S PAYMENTS STRATEGY

The $4.4 billion acquisition of CheckFree in 2007 "was the beginning of [Fiserv] becoming a payments company."

—**DEVIN MCGRANAHAN**, EXECUTIVE VICE PRESIDENT, FISERV

Fiserv Inc.'s acquisition of First Data Corp. this year was the first of a trio of big mergers that has made 2019 the year of the megadeals in payments. Recently, a key Fiserv executive close to the action explained how the $22-billion acquisition served as the capstone to a long-term strategy at Fiserv to transform itself into a major payments company.

"In 2018, we launched the first enterprise payments strategy for Fiserv. We began to think of the company almost entirely as a payments company," said Devin McGranahan, a 20-year veteran of McKinsey & Co. who joined Fiserv's management ranks in 2016 and now serves as executive vice president and a senior group president for payments.

But the groundwork for that strategy had been laid 12 years ago, McGranahan explained, when Fiserv acquired CheckFree, an early entrant in electronic bill pay, for $4.4 billion in cash. He was close to the company's strategic thinking even then as an advisor. "That was the beginning of us becoming a payments company," he told the audience in September at the Electronic Transactions Association's Strategic Leadership Forum in Boca Raton, Fla.

By last year, the long-term strategy was nearly complete—but for one key component. "In 2018, we realized we were missing an important element, commerce, or merchants," McGranahan told the audience of top payments-industry professionals. With more than half its operating revenue derived from merchant acquiring, and with some 6 million merchants in its portfolio, that was a gap First Data was eminently qualified to fill.

Now, Fiserv is bent on blending First Data's capabilities with its historic strength in core-account processing, a vital but unflashy business. "It's hard to differentiate core processing," McGranahan said. In this respect, the technology acquisitions First Data had made were of prime interest, he added.

First Data's smart-terminal business, Clover, particularly appealed to Fiserv. So did CoPilot, a portfolio-management portal created by CardConnect, a merchant-services provider First Data bought in 2017. "We have the largest bill-pay platform in North America. We have Clover and CoPilot. How do we integrate bill-pay into the Clover platform, for example, and stitch these companies together to add value?" McGranahan asked.

Clover, which First Data acquired seven years ago, now features more than 400 commerce apps. First Data last year reached 1 million shipments of the device, according to Bala Janakiraman, a First Data executive vice president who shared the stage with McGranahan.

The next step, both men said, is to adequately fund new payments features under the Fiserv banner. To that end, the company is dedicating $500 million to innovation, Janakiraman said.

—John Stewart

AN ISO'S $135-MILLION WIN AGAINST GLOBAL PAYMENTS

Global Payments Inc. may be on the hook for more than $135 million following a jury verdict in a breach-of-contract lawsuit filed by an independent sales organization against the Atlanta-based processor.

A jury in the Superior Court of DeKalb County in Georgia found that Global Payments breached parts of its merchant-service agreement with Frontline Processing Corp., a Bozeman, Mont.-based ISO. The jury on Sept. 23 awarded the ISO more than $24 million in direct damages and $109.8 million in consequential damages. It also awarded Frontline more than $1 million to cover its costs and attorney fees. Judge Linda W. Hunter signed the judgment Sept. 30.

Global Payments intends to appeal the decision. "We believe this case is completely without merit and will appeal it immediately," says a statement from the processor. "The outcome is inconsistent with the facts and well-settled law, and we fully expect to prevail on appeal. We will not stop until this gross miscarriage of justice is reversed."

Frontline filed the suit in 2015 after Global Payments withheld funds to cover its legal costs in a lawsuit the Consumer Financial Protection Bureau brought against the processor and two ISOs, Frontline and Pathfinder Payment Solutions Inc., for allegedly providing payment services to malicious merchants. That case was dismissed in 2017.

Pathfinder was dismissed by the DeKalb County court as a plaintiff in 2018 when it could not provide an attorney to represent it, says Joe Gleason, Frontline co-counsel and partner at Atlanta-based Gleason Law LLC.

The dispute between Frontline and Global Payments actually preceded the CFPB action, Gleason tells *Digital Transactions.* In 2013, Frontline and Global Payments were negotiating to extend their contract, but Global Payments wanted to add terms that Frontline was not willing to agree to, Gleason says.

In 2014, after shopping around, Frontline agreed to a similar deal with First Data Corp. and told Global Payments it would stay if it could match First Data's pricing. "Global did not match the pricing," Gleason says.

Under Frontline's agreement with Global Payments, merchants that Frontline refers to the processor are portable. Global Payments would not allow that, Gleason says, making it one of the breach claims.

"Then the CFPB case comes along and becomes a convenient excuse to destroy Frontline by withholding Frontline's funds, by withholding merchant-reserve funds, by locking Frontline out of Global's computer systems," Gleason says. That effectively cut Frontline out of the picture, he says, placing Global in direct dealings with the referred merchants, another breach allegation.

"In our view, the breach-of-contract cases did not start with the CFPB lawsuit," Gleason says. "Instead, it was just one more step."

Frontline contended that neither the merchant-services agreement nor referral agreement the ISOs had with Global Payments allowed the processor to "deduct as expense or withhold from compensation owed to Pathfinder or Frontline Global's legal fees incurred in defending itself in the CFPB action."

—Kevin Woodward

MONTHLY MERCHANT METRIC

Total Gross Processing Revenue, in Percent

Sum of total discount, total transaction fee revenue, and total other fee revenue divided by total volume

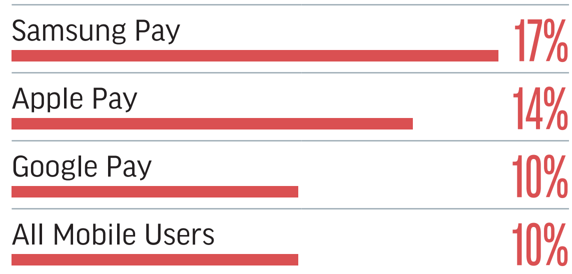
Note: This is sourced from The Strawhecker Group's merchant data warehouse of over 3 million merchants in the U.S. market. The ability to understand this data is important as small and medium-size businesses (SMBs) and the payments providers that serve them are key drivers of the economy. All data are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

Payments Experts. Powerful Data. THE STRAWHECKER GROUP

SAMSUNG PAY MAKES ITS MOVE(S)

MOBILE REMITTANCE

(Percentage of users who had a need to send or receive a money transfer internationally in the past 18 months)



Source: Auriemma Consulting

Adoption of mobile-payment apps in the United States has been tepid, so the so-called "Pays"—Apple Pay, Google Pay, and Samsung Pay—are seeking new features to spike consumer interest. The latest gambits come from Samsung Pay, which last month announced a digital prepaid card called Samsung Pay Cash and an integration that will allow U.S. users to send payments to overseas recipients.

The new Money Transfer feature, which comes through a collaboration with cross-border payments specialist Finablr PLC, is available so far only in the U.S. market, but will expand to more countries next year, Samsung Pay says.

The company says users can send money "in most major currencies" from any credit or debit card they've stored in the app to recipients in 47 countries, without leaving the app. They can also see within the app all fees and exchange rates connected to each transfer. Recipients can get their money via several methods, including deposit to bank accounts and cash pickup.

The service relies on capabilities from Travelex, a unit of Finablr and a long-time provider of international money services.

Launched in 2015, Samsung Pay claimed 9.9 million U.S. users for proximity payments last year, trailing Apple Inc.'s Apple Pay at 22 million and Alphabet Inc.'s Google Pay at 11.1 million, according to eMarketer.

Now the growing market for international transfers could spark more adoption and usage for Samsung Pay. Overall remittances grew 8.8% in 2017, to $633 billion, according to the World Bank. Payments-research firm Aite Group forecasts that figure will reach $739.2 billion by the end of next year. Digital transfers are already between 10% and 15% of the total, up from 7% in 2016, the firm estimates.

Experts who follow mobile payments see Samsung Pay's remittance gambit paying off, though estimates of how much vary.

"This is a major development in the mobile-wallet space, and one that competitors will be pressed to match," says Aaron McPherson, vice president for research operations at Marlborough, Mass.-based Mercator Advisory Group, in an email message. "The availability of the Travelex network is particularly important, as is the ability to do cash-out transactions."

Some aspects of the new service, however, have yet to emerge and could prove critical. "We still need details such as cost and speed of settlement, but based on what has been announced, it looks very appealing," McPherson says.

Among mobile-wallet users, Samsung Pay aficionados may be particularly drawn to international transfers. While only 10% of all mobile-pay users said in an Auriemma Group survey this spring that they had needed to send or receive a payment to or from another country within the past 18 months, the fraction for Samsung Pay was highest at 17%. Only Apple Pay, at 14%, approached that number (chart).

While the market may be limited, "it seems there's definitely opportunity for Samsung Pay to capture some of the [peer-to-peer] and traditional remittance-services market share, among that small group of consumers," says Jaclyn Holmes, director of research at New York City-based Auriemma.

At almost the same time, Global Payments Inc., the big Atlanta-based processor that recently acquired Total System Services Inc. (TSYS), said it has now integrated technology enabling Samsung Pay Cash's virtual prepaid Mastercard into Samsung's wallet.

The technology comes from Netspend Corp., a company Global picked up as part of its $26.1-billion deal for TSYS. Global also announced Mastercard Inc. is providing tokenization service for Samsung Pay Cash, a move intended to mask the

NORTHEAST ACQUIRERS ASSOCIATION
CELEBRATING 35 YEARS

2020 NEAA CONFERENCE & TRADE SHOW

is back in Boston!

February 5th- 6th, 2020

Boston Marriott Copley Hotel

Join us in historic Boston for our 35th Anniversary Event. Attracting the best and brightest in payments.

NEAA 2020 is sure to be our biggest event to date.

- **Pertinent educational sessions including hot topics like cash discount/surcharging and cannabis/CBD**
- **Extended expo hours to showcase products and services that are shaping our industry**
- **Two days of peer networking**
- **Don't miss Catapult 2020 – our annual innovation, technology competition**
- **Accomplished speaker roster delivering impactful insights on today's trending topics**

Register for NEAA 2020 and book your hotel today for special pricing.
Register at www.northeastacquirers.com

Created by: USAePAY

digital card's actual credentials as users perform transactions.

Samsung Pay Cash is aimed at "a variety of use cases," Global's announcement says, most especially spending and budgeting. Devices that can run Samsung Pay include Samsung models S6 and later.

Users can load the virtual card via a credit or debit card already in the Samsung Pay app or an automated clearing house transfer from an existing bank account. Users can then rely on the new card to make payments at any location that accepts Samsung Pay and Mastercard.

—John Stewart

PAYMENTS DOMINATE FINTECH M&A

Payments are popular with investors this year, with mergers and acquisitions involving payment processors ranking as some of the biggest deals in the financial-technology sector in 2019's first three quarters.

An October analysis by New York City-based investment bank Berkery Noyes Securities LLC says payments firms were involved in four of the top 10 fintech M&A deals (chart). The value of the payments mergers totaled \$94.2 billion, or 72% of the \$130.9 billion total valuation of the 10 deals.

TOP 10 FINTECH DEALS OF 2019

	TARGET COMPANY	BUYER	VALUATION (in billions)
1	Worldpay	FIS	\$42.9
2	Refinitiv	London Stock Exchange Group	\$27.0
3	TSYS	Global Payments	\$26.1
4	First Data	Fiserv	\$22.0
5	Ellie Mae	Thoma Bravo	\$3.31
6	Nets	Mastercard	\$3.19
7	Assurance IQ	Prudential Financial	\$2.35
8	iPipeline	Roper Technologies	\$1.63
9	eFront	BlackRock	\$1.30
10	Tranzact	Willis Towers Watson	\$1.20

Source: Berkery Noyes

Note: Mergers and acquisitions announced in year's first nine months.

Four of this year's mergers were valued at more than \$20 billion, compared with none in 2018, and three of them involved payment processors. The \$42.9 billion July acquisition of processor Worldpay Inc. by Fidelity National Information Services Inc. (FIS) topped the list. In third place was Global Payments Inc.'s \$26.1 billion September buyout of Total System Services Inc. (TSYS) ("How the Global-TSYS Deal Is Different," July).

The No. 4 deal was Fiserv Inc.'s \$22 billion July acquisition of leading processor First Data Corp., the transaction that started the payments dominos falling.

Mastercard Inc.'s planned acquisition of a major part of Danish processor Nets Group's operations, announced in August and expected to close next year, is valued at \$3.19 billion and ranked sixth. "The most active acquirer year-to-date was Mastercard with five acquisitions," the report says.

Two of Mastercard's acquisitions came in the third quarter, Nets and bill-pay platform provider Transactis Inc. ("The Networks' Shopping Spree," September).

Several of the other Top 10 mergers involved insurance or financial companies. In all, Berkery Noyes tracked 436 deals in 2019's first three quarters, up nearly 14% from 384 in the same period last year. The total value of the transactions more than tripled to \$151.3 billion from last year's \$42.5 billion.

The median revenue multiple to enterprise value was 3.4 times compared with 2.9 times in 2018, according to Berkery Noyes. DT

—Jim Daly

THE AGE OF INSECURITY

BY GIDEON SAMID
gideon@bitmint.com

THERE ARE HUNDREDS of cybersecurity companies offering products designed to protect us from identity theft by requiring us to prove our identity through biometrics and unscripted behavior.

These products claim efficacy against today's threats. Many of them even grow and prosper as they defeat a great deal of contemporary fraud. The problem, though, is that the cyber threat is about to leapfrog into new dimensions that will overwhelm today's cyber defense. The lethal combination of artificial intelligence and "Deep Fake" will create phony remote identities so convincing that your mother would be fooled.

I'll get to Deep Fake in a moment. Artificial intelligence, or AI, can study a person's behavior, identify an underlying pattern, and use this pattern to mimic that person's behavior with stunning accuracy. AI keeps improving. Soon enough, all the many products that identify intruders and fraudsters through their behavior will be outsmarted by AI engines that grow increasingly faithful to the behavior of their victims.

Deep Fake technology takes a still picture of a person and constructs a believable video of that person talking and moving. Put this technology together with AI, and you face a threat of unprecedented proportions. Each of us could be seen on a fake video speaking with our characteristic voice and reacting in ways that convince even those who know us intimately that what they see is authentic.

Some even theorize that criminals could dispose of some individuals and then build virtual replacements of the "evaporated" persons, each committing crimes. If the fraud is discovered, there is no one to hold accountable.

I'm drawing this to your attention, but I fear a column like this will not shake up our cyber defenses. I've come to realize that security measures are often either for show or for providing a plausible defense when breached. Or they're a panic-driven counter measure that's burdensome, expensive, and inefficient.

Still, let's look at some effective counter measures.

The key principle for tomorrow's cyber defense is "physical anchorage." Let's use an aviation analogy: planes fly high and fast for long hours and in all sorts of weather—but they all took off from a tarmac, and after doing their business in the air they all land on terra firma. Cyberspace is the plane. It must take off and land in a physical reality.

Take a look at networks where nodes can be freely formed and claimed to be distinct individual entities. You will find fraud, fake news, trolls, and so on. Blockchain technology will not cure this affliction. Networks where nodes need to prove their identity offline, and then reaffirm it when they leave the network, are much more secure.

The growing use of biometrics reflects this trend toward physical anchorage for cyberspace. The skin of your thumb expresses data non-digitally, and it is up to us how many bits to use to represent it. In other words, chemistry is an inexhaustible source of digital data. The big issue with biometrics, though, is that once your fingerprint is compromised, it is forever compromised.

New technologies promote artificial biometrics, where people will use a manufactured "finger," which is activated by its owner's biometric, but where the data sent to the cloud is from the replaceable "finger." The biometric verification is done locally in the manufactured finger. It is not transacted over the Internet.

Networks will mushroom over a skeleton construction where communication is transacted between physical stations that are smart enough to destroy their content when tampered with.

In this way, the integrity of the future cyberspace will depend on mooring it to the physical space at multiple contact points. DT acquiring

THE ABCs OF CBD

Some ISOs are high on selling acceptance services to marketers of this hemp derivative. The profit potential could be big, but so are the complications.

BY **KEVIN WOODWARD**

THE POTENTIAL PAYOFF from high-risk CBD merchants is stoking the acquiring industry's enthusiasm.

Almost a year after the passage of the 2018 Farm Bill that legalized the cultivation and sale of hemp-derived products at the start of this year, the acquiring industry's efforts to add CBD-selling merchants to their portfolios have been growing.

The potential for large profit margins from these high-risk merchants is motivating many independent sales organizations and acquirers to sell merchant services to them—or at least to consider how it might be done. CBD, the shortened name for cannabidiol, is an ingredient that is derived from hemp but causes no high. CBD's popularity as a treatment for everything from pain to anxiety has exploded in the past year.

The product's appeal for acquirers, however, is not without caveats. Issues payments providers may encounter include securing an acquiring bank that accepts CBD merchants, complying with payments and governmental regulations, and evaluating and then monitoring CBD merchants once boarded.

"The banks are having a tough time now because it's so new," said Travis Chrisman, president and cofounder of Coastal Pay, a Carlsbad, Calif.-based independent sales organization. Speaking in September at the Western States Acquirers Association annual conference in Rancho Mirage, Calif., Chrisman said underwriting guidelines are challenging for banks.

"CBD is the largest emerging market in the world," said Chrisman. "There's a lot of attention. A lot of people are wanting to jump in." While boarding CBD-selling merchants may be profitable, the challenges to getting there are many and complex. "The biggest factor is banking," Chrisman said.

The challenge is understanding merchant services for CBD sellers, said Jason Putnam, senior vice

DigitalTransactions.net

The payments market, all in one place.

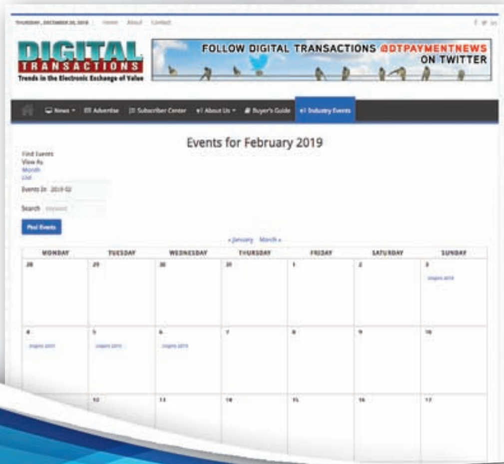
Breaking news from the payments market, posted daily

Concise, clean interface is easy to navigate

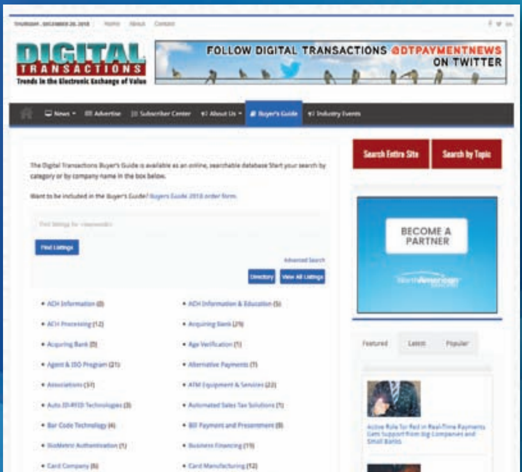
13 years of payments news and analysis

Complete current and past issues of *Digital Transactions* magazine

Calendar of industry events



Detailed listings of payments market suppliers



DIGITAL TRANSACTIONS

Trends in the Electronic Exchange of Value president and director of merchant services at Farmers Branch, Texas-based The Independent Bankers Bank N.A. The banks not only have to evaluate the merchant, they have to do so from the perspective of complying with their regulators, such as the Office of the Comptroller of the Currency, he said.

"We have to be on par with the regulators and we have to make sure they understand what's going on," Putnam said. "We want to help our banks do this." As a banker's bank, TIB provides correspondent-banking services to more than 1,600 independent community banks.

Regulators like when banks adhere to a standard because it can facilitate compliance, he said, adding, "The biggest thing is making sure the regulators are OK with how we handle this."

Putnam says his bank is evaluating merchant services for CBD-selling merchants, but it has not "stepped into this world."

'It will just get better and better.'

—**TRAVIS CHRISMAN**, PRESIDENT AND COFOUNDER, COASTAL PAY

The appeal of these merchants for banks and acquirers is largely rooted in the profit potential. "If they can overcome the risk aspect, if they can explain what the scenario is, they would be very comfortable," Putnam says of bank interest.

That interest is apparently high in many sectors. "I've never seen anything like this," Todd H. Halpern, a partner at Venable LLP, a Washington, D.C.-based law firm. "I have never seen so much hype over a single ingredient with so many potential applications in food, cosmetics, and not just dietary supplements."

In addition to banking regulation, there are other legal issues to consider. "From a legal perspective, the issue of the legality of CBD continues to be complicated," says Andrew E. Bigart, also a partner at Venable.

'BE REALLY CAREFUL'

While CBD products sit astride several legal issues, the major one is that the 2018 Farm Bill removed hemp, but not cannabis, from the controlled-substance list, Bigart says. There is a complicated legal definition of hemp and products derived from it, but for payments providers the primary requirement is that CBD products contain no more than 0.3% THC, the high-producing ingredient in marijuana. And they must originate from hemp plants, not marijuana ones.

"The significance of the Farm Bill was that it created an exemption from the definition of marijuana for 'hemp' which is defined in the statute," Halpern says. "To be hemp, the cannabis plant that is the source of the product must have a THC content of no more than 0.3%. That's important because it's the beginning of the analysis to determine if the CBD product being sold is lawful."

Related legal issues have to do with the liability associated with not meeting Drug Enforcement Administration and Food and Drug Administration regulations. Another complication arises from litigation over false advertising, which can come from the Federal Trade Commission, state attorneys general, or private lawsuits, Halpern says.

Further complicating the boarding of CBD-selling merchants is that these products are not legal in all 50 states. Though the 2018 Farm Bill created a category of hemp and exempted it from federal definitions of a controlled substance, the bill did not pre-empt state definitions. "It's important for banks and payment processors and their merchant-service providers to understand that legal framework," Bigart says.

And, once the merchant is boarded and actively selling CBD products, the acquirer's job is still not done. As with many high-risk merchants, the acquirer must monitor the merchant to ensure it adheres to the stipulations of the merchant-services agreement. This may also be an issue for existing merchants that add CBD products to their inventory.

In these agreements, Halpern suggests including the ability to get as much information as possible from the merchant to get the necessary oversight and increase the flexibility to terminate the relationship if necessary. This is particularly important if the legality of CBD changes or there are changes in the interpretation of the law.

"You need to be really careful as acquiring banks that the THC level is below the guidelines," Sharon Lampley, Mastercard Inc. director of acquirer-channel management, said at the WSAA conference.

Another complication: the merchant may be located in a state that allows CBD sales, but may sell online into a state that doesn't, Lampley says. CBD is illegal in South Dakota, for example. Such sales constitute interstate commerce, which is governed by federal regulations.

'LITTLE THINGS'

Another factor for ISOs and acquirers to weigh is that there are no merchant category codes for merchants selling CBD products, Lampley says. The MCC is assigned to the merchant type. A gym that sells CBD products would be assigned the MCC for a gym.

And, just as with any other merchant, the merchant-services provider has to consider how to monitor the merchant to ensure violations of card-brand rules do not occur, Lampley said.

Lampley suggested acquirers monitor what their CBD merchants sell. "It's all of these little things you have to be aware of as an ISO and the merchant you're bringing on," she said. The key for growing this business is consistency in standards, she said. "We continually look at this environment. As it grows and becomes more consistent, we can change our rules accordingly."

But merchants aren't absolved of responsibility. Card-brand penalties for noncompliance can run into the thousands of dollars. Merchants also may face legal issues on their own. Merchant processor Square Inc., which announced a CBD program in October, says generally that it monitors its sellers closely for compliance.

> 'I've never seen anything like this.'
> —**TODD H. HALPERN**, PARTNER, VENABLE LLP

For example, the San Francisco-based company conducts "enhanced due diligence," but didn't say what that involves. The review ensures sellers meet CBD-specific obligations, Square says, and it requires them to attest to and be responsible for local, state, and federal law compliance.

Square's prices are 4.2% plus 30 cents per online and in-app transaction. In-person fees are 3.9% plus 10 cents for tapped, dipped, or swiped transactions. Keyed and card-on-file fees for CBD sellers are 4.8% plus 15 cents.

'THIS WILL BE HUGE'

Though Coastal Pay does not post its CBD pricing online, Chrisman says an agent could make about 100 basis points. A basis point is one-hundredth of a percent.

Coastal Pay asks CBD-selling merchants for the typical documentation associated with a high-risk merchant account, Chrisman says. That may include six months of card-processing statements and three months of bank statements, plus verification the merchants have valid certificate-of-analysis certifications that indicate an accredited laboratory tested the amount of CBD in each product.

Courting and boarding merchants that sell CBD products is very complex and bound to evolve through the sheer impact of regulation and competition. But that's not enough to deter some.

"This will be huge," Chrisman says. "It will just get better and better." DT

13TH ANNUAL

THE 10 MOST PRESSING ISSUES IN E-PAYMENTS

What's keeping you up at night? If you said nothing, you're lucky. Here's a list of the biggest issues troubling most payments executives today.

BY JIM DALY, KEVIN WOODWARD, AND JOHN STEWART

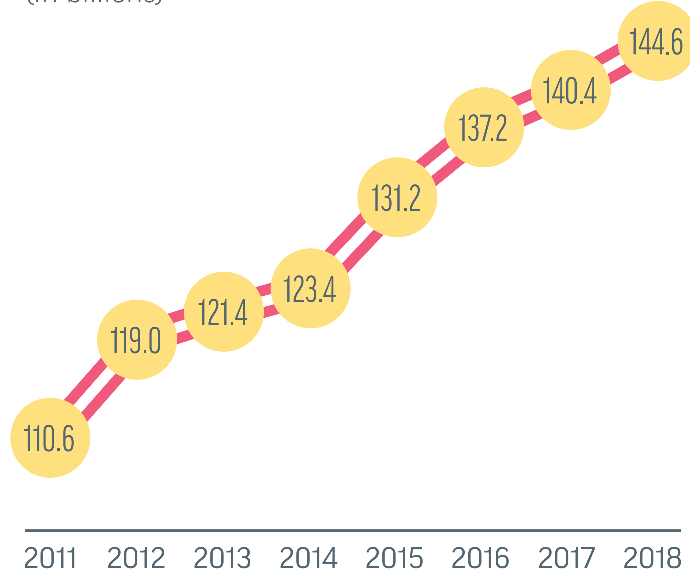
WE LIVE IN A WORLD FULL OF TRIBULATION AND TURBULENCE, and the payments business is no exception. Herewith, we offer our annual catalog of the 10 biggest issues the industry faces today. We wish we could offer easy solutions, but hard problems are hard precisely because they admit no easy answers.

Still, we contend it's useful to face these issues squarely, to round them up in a list like this and dig into them a bit. If you agree, you may find this list a useful start toward confronting and solving issues in your shop. We hope that's the case. If you disagree … well, it's a free country.

At any rate, if you think we've omitted something just as pressing as the items on this list, please let us know and we'll consider it for next time. Just shoot me an email at john@digitaltransactions.net. Meanwhile, may all your problems prove solvable—and if they do, please let us know how you did it!

Consumer Electronic Transactions in the U.S.

(In billions)



Note: Figures include all consumer-based card and ACH volume. Source: Digital Transactions estimates

1. NO SOLUTION for DATA BREACHES?

There are now three, not just two, certainties in life: death, taxes, and data breaches. Despite 13 years of PCI security standards and ever-increasing attention and money spent toward preventing and mitigating data breaches, they just keep on coming.

Risk Based Security Inc. says data breaches are on a record-setting pace this year. The data-protection analytics and consulting firm tallied 3,813 breaches in 2019's first half, up 54% from a year earlier. Those breaches exposed more than 4.1 billion consumer records, up 52% from 2018. Of course, many compromised records are not payment card or bank-account numbers and related data, but millions still are.

There is some good news. Visa Inc. recently reported that for merchants who had completed their EMV point-of-sale terminal upgrades, dollars lost to counterfeit fraud—the bane of magnetic-stripe payment cards—had dropped by 87% as of March compared with September 2015. Over the same period, Visa says counterfeit fraud dollars lost by all U.S. merchants fell 62%, and Visa's overall card-present fraud rate declined by 40%.

The payment card networks' October 2015 EMV liability shifts transferred responsibility for counterfeit fraud to the merchant if a POS terminal couldn't read an EMV card's chip.

Fraudsters intent on counterfeiting credit and debit cards need supplies of card data typically stolen in data breaches. So while counterfeiting is in a steep decline as mag-stripe cards go away, data breaches continue because the demand for card data has not gone away. The data simply is being used for more online fraud and variations of identity fraud. So, sadly, breaches will continue for the foreseeable future.

2. E-COMMERCE FRAUD

There's nothing new about the scourge of fraud in e-commerce markets. The difficulty in vetting users has always meant losses here are higher than in physical stores.

And the cost doesn't stop with the purloined merchandise. Total costs—including mitigation efforts—are highest among mid-to-large e-commerce merchants, according to Alpharetta, Ga.-based Lexis Nexis Risk Solutions. The firm's latest "True Cost of Fraud" report, released in September, found each dollar of fraud costs these sellers $3.50, higher than in any other category of merchant studied.

There are multiple reasons for this, but in general online merchants have been easier pickings for fraudsters because it's harder to verify identities online. Indeed, LexisNexis blames synthetic IDs, automated bot attacks, and ID-verification challenges for an overall increase in fraud attempts against all merchants.

In response, the global card networks are ushering in two major technologies. One of them, called 3-D Secure 2.0, is the second generation of an older technology aimed at simplifying the process of making sure users are who they say they are. The other, called Secure Remote Commerce, has a twofold aim: securing transaction data with tokens and streamlining checkout flows with a single buy button.

SRC is expected to go live with most networks by the end of the year, and processors are already lining up to introduce 3-D Secure 2.0. Amsterdam-based payments gateway Adyen N.V., for example, is rolling it out across Europe ("Europe's All-Embracing Regulations," page 24) and expects to launch it in the United States next year.

The big drawback with the first version of 3-D Secure was that it complicated transactions, leading many merchants to abandon it. Will the new version be less forbidding? With SRC, some merchant groups are concerned about how the tokenization process will affect their transaction-routing rights under the Durbin Amendment. Networks like Visa and Mastercard say those rights will be respected. It remains to be seen whether merchants will buy that.

3. AUTHENTICATION: CONFUSION at the POS

Merchants have long wanted to ensure the consumer conducting a payment transaction at the point of sale is who she says she is. With streamlined options—think mobile wallets and biometrics—merchants have access to digital verification techniques. But one stalwart, the signature, continues to persist despite card-brand changes that made signature authentication optional for EMV-accepting merchants.

A year ago, a National Retail Federation survey found that 40% of retail executives planned to drop signature requirements for payment card transactions. Without data, it's unknown how many merchants continue to ask for a signature when it's not necessary.

Efforts to move even farther from signature authentication at the point of sale progressed with the release this summer of the Apple Card. This digital-centric credit card sequesters all of the card information—full card number, expiration date, and card verification code—in the companion iPhone wallet. The Apple Card also eschews a signature panel.

The Apple Card is among the first credit cards to make such a drastic push for digital authentication, especially for e-commerce transactions. "Apple Card is a step in the right direction from a data-security standpoint," Jordan McKee, research director at New York City-based 451 Research, says in an email. "The go-forward goal of the industry should be to eliminate the usage and visibility of sensitive data wherever possible."

The reliance on Apple Wallet to house confidential payment information for the card won't change how payment data will be processed and stored for transactions, says Krista Tedder, director of payments at Pleasanton, Calif.-based Javelin Strategy & Research.

"What will change is the authentication approach used to authenticate the payment, store the credentials for subsequent usage, and how the consumer can access the information," Tedder says. "Leveraging Apple Pay or other stored-credential applications, which require additional authentication, such as device fingerprinting, biometrics, or other tools, meets multifactor authentication guidance that the industry is moving towards."

4. FedNow's IMPACT ON REAL-TIME PAYMENTS

Until August, everything seemed to be cooking along for real-time payments in the United States. That's when the Federal Reserve, which had been hinting for months that it might get involved, jumped into the game with both feet. Now observers are fretting that the newly christened FedNow real-time payments effort, which isn't supposed to begin operating until 2023 at the soonest, could slow the momentum that had been building for blink-of-an-eye payments processing.

Much of that momentum has been the result of a real-time service rolled out in 2017 by The Clearing House Payments Co. LLC, the New York City-based automated clearing house and wire operator owned by 24 of the nation's biggest banks. By this fall, TCH's RTP service had connected to just over half of the nation's accounts for real-time receipt.

Mid-size and small institutions are said to welcome the public option offered by FedNow as a counterweight to the private-sector service from TCH. Some bankers worry that, with only TCH to turn to, pricing will skyrocket. But others are concerned that waiting for FedNow to go online four or five years from now will only slow progress in the United States toward the long-held goal of real-time payments.

Meanwhile, the RTP service, built on technology from Mastercard Inc.'s Vocalink unit, is still signing up customers. In September, New Jersey's Cross River Bank was the latest.


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

5. The EMV Fuel-Pump CONVERSION LOOMS

Even with three additional years beyond the original liability shift for EMV transactions, the petroleum-industry outlook for full EMV compliance is not good.

With its original compliance date of October 2017 postponed to October 1, 2020, the fuel-retailing industry's EMV conversion for in-store transactions has progressed well. A recent survey from Conexxus, an Alexandria, Va.-based information technology association, found that 86% of those surveyed reported full EMV compliance inside their stores. It's at the pump where the challenge looms. Here, only 13% said they have contact EMV deployed.

The good news, especially with a year to go, is that 80% of those without EMV at the pump planned to implement it. The big impediment is software. Fifty-two percent said the lack of available software stood in the way. Only 42% said that they are or will be 100% compliant by the 2020 date. One-fourth did not know when they might be ready.

The extra time for EMV at the pump appears to have been very necessary, especially as vendors prepare EMV-compliant products. One, Gas Pos, launched a service that puts EMV-compliant card readers in fuel dispensers and in convenience stores, all of which are connected to a fuel controller.

Citgo Petroleum Corp. released its EMV-acceptance Passport software, provided by Gilbarco Veeder-Root, this summer. Gilbarco, in conjunction with Chevron Corp., developed a trade-in program for retailers to get EMV-compliant equipment. And Wayne Fueling Systems LLC launched an online EMV resource center for c-store operators.

The work will prove essential. Already aware of EMV at the point of sale, consumers have a heightened perception of payment security. Sixty-two percent of U.S. adults in an ACI Worldwide survey from earlier this year said they were concerned about the security of their financial data when making a payment at fuel pumps.

6. Merchant Account ATTRITION & RETENTION

Not only is merchant retention valuable to acquirers for the immediate needs of generating revenue, but as competition incessantly intensifies, strategies to support lower attrition have a long-term value.

Reasons for this are many. ISO executives looking for an exit by selling their entire portfolio will get higher multiples on revenues if their merchants are spread across multiple industries, and the portfolio has relatively low attrition, according to Jon Engleking, chief operating officer at Super G Capital LLC. "The buyers are looking for a well-balanced portfolio," he said. "You're going to get a higher multiple the more diversified your portfolio is."

A buyer may view a balanced portfolio with a lower attrition rate relative to another as the better acquisition.

Retaining merchants, though, is a daunting challenge. The industry's concerted effort in the past few years with cloud-based point-of-sale systems directly aims at this issue. Such POS systems can be a hub for all of a merchant's data, not just for enabling and tracking its payments. Even online payments companies are getting into the point of sale. Stripe Inc. added in-store payment software for certain countertop devices its merchants can use.

"While we mostly focus on Internet businesses, 90% of consumer spending still takes place in person," Devesh Senapati, product manager for Stripe Terminal, said in a blog post.

One piece of advice when using cloud-based POS systems and integrated software in this way is to start by pitching it to the existing merchant portfolio, says Pierre-Emmanuel Perruchot de La Bussière, vice president of business development and partnerships at Vend Ltd., a New Zealand-based POS-system developer with offices in San Francisco.

Trying to sell a new solution to existing merchants "might be the better idea," he says, because the sales organization already has an established relationship with the merchant and doesn't need to forge that simultaneously with a sale.

7. Discounting & Surcharging: CONFUSION PERSISTS

Merchants are always interested in reducing their payment card acceptance costs, and two ways to do that are by adding a surcharge for card payments or by giving customers a discount if they pay with cash. Thus, surcharging and cash discounts have been hot topics for several years now at regional conferences for independent sales organizations.

Despite all the educational sessions, implementing surcharging and cash-discount programs properly remains a confusing and sometimes perilous task for ISOs and their merchants, who must abide by network rules governing the programs or risk losing their card-acceptance privileges.

While surcharges require proper notifications and have other requirements, cash discounts can be especially troublesome to implement and are "one of the most misunderstood programs" for merchants, one merchant-acquirer executive said at a conference this year. Critics say cash discounts frequently are just surcharges in disguise because merchants often raise prices before applying the discount.

Cash discounts generate questions partly because of a paucity of network rules governing them compared with surcharges, one acquiring executive on a conference panel noted. One key requirement is that only credit card sales can be surcharged.

Confusion about rules governing cash discounts became so widespread that Visa Inc. a year ago issued reminder guidance to the acquiring community. Acquirers are charged with enforcing Visa and Mastercard Inc. network rules.

Some ISOs remain enthusiastic about surcharging and cash-discount programs because of their high margins. Relatively few merchants have implemented either cash discounts or surcharges so far, but expect more if margins remain high—and the networks don't crack down.

8. Can Anyone Ever Get Away With CHARGING for P2P PAYMENTS?

The good news for payments companies is that person-to-person payments are wildly popular. But that's also the bad news. The reason? For the most part, P2P payments are free to users. Two of the country's biggest networks, PayPal Holdings Inc.'s Venmo and Early Warning Services LLC's Zelle, charge users exactly zero for each payment.

That's costing the networks a lot of foregone revenue. PayPal, for instance, reported in July that Venmo's volume soared 70% in the second quarter to $24 billion. But the free transfers helped knock the company's take rate—the percentage it keeps on each transaction—down 13 basis points to 2.25%. Early Warning faces much the same problem with its $44 billion in quarterly Zelle volume. So does any outfit offering P2P these days.

How to solve the ironic problem of overwhelming popularity for a free product that the market expects to remain free? PayPal has promoted fee-bearing services based on Venmo, like instant withdrawal, a Venmo card, and Pay With Venmo, an e-commerce service. On these services, some 1.5 million Venmo users performed a "monetizable" transaction in the second quarter, PayPal said, letting the company draw user or merchant fees. The instant withdrawals alone account for about half the take.

Will that work for everyone? Time will tell, but for now the best things in life—including P2P payments—remain free.

9. CAN Private-Label Wallets SURVIVE?

Most observers would agree that while they have yet to set the world on fire, the general-purpose mobile wallets often called "the Pays"—Apple Pay, Google Pay, and Samsung Pay—are likely to be around for a while. Apple Inc. claims Apple Pay is on track to hit 10 billion transactions this year. Samsung Pay just added an international money-transfer service and a virtual prepaid card, and Google continues to integrate Google Pay with its many other services.

Meanwhile, consumers have embraced a handful of mobile wallets offered by individual merchants, particularly Starbucks and Dunkin'. And Walmart continues to enhance the Walmart Pay service within the Walmart app.

The same can't be said of the bank mobile wallets that began appearing at mid-decade. Only a few big banks—most notably Chase, Citigroup, Capital One, and Wells Fargo—offered them, and they functioned as private-label alternatives to the Pays. Customers could load credit and debit cards from those banks into the wallets to pay where Visa and Mastercard mobile payments were accepted.

Despite having tens of millions of customers, though, the banks' smart-phone payment apps failed to catch on with consumers. Cap One and Wells quietly folded their wallets last year, and Citi shuttered its Citi Pay service Aug. 31.

The biggest blow came when Chase, the nation's largest credit card issuer and provider of the Chase Pay mobile wallet, said in August that it would discontinue the app in early 2020. The Chase Pay service, however, will carry on as a payment option on merchant Web sites that display its logo and through merchant apps, as well as through PayPal. And some Chase Pay features are now in the Chase banking app.

Thus, while the Pays and the mobile wallets of a few dedicated merchants seem likely to survive, not so for standalone payments apps from banks. Observers say banks would be better off improving their mobile-banking apps rather than competing head-to-head with the Pays. "The days of bank-branded wallets are coming to an end," says payments analyst Jordan McKee of New York City-based 451 Research.

10. REAL-TIME Payments and the ACH

The growth of real-time payments, especially since the Federal Reserve proposed its FedNow real-time gross settlement service in August, has generated a tide of questions ("The New Reality in Real-Time Payments," September). Among them are the possible effects of real-time payments on the nation's automated clearing house network.

Once considered a massive but dull backwater of payments, the ACH in recent years has adapted to changing technologies and merchant and consumer demand with new transaction categories and speedier settlement.

ACH governing body Nacha rolled out same-day ACH settlement in 2016, and same-day transactions now number more than 1 million per day. In September, a requirement for faster funds availability took effect. Next up is an increase in same-day transaction dollar limits, from the current $25,000 to $100,000, set for March. Extended operating hours are planned for a year after that.

What the ACH needs to do to stay competitive in a rapidly changing market for faster payments is a matter of debate. In written comments for September hearings by U.S. House and Senate committees probing faster-payments issues, Nacha noted that the ACH, for which The Clearing House and the Fed are the two U.S. operators, already is a model of interoperability—a key issue as faster-payment systems proliferate.

But Nacha said the payments industry needs more from the Fed than just FedNow, especially expanded hours of operation from the Fed's National Settlement Service. DT

USPS STATEMENT OF OWNERSHIP, MANAGEMENT AND CIRCULATION

1. Publication Title: **Digital Transactions**
2. Publication Number: **024-247**
3. Filing Date: **October 9, 2019**
4. Issue Frequency: **Monthly**
5. No. of Issues Published Annually: **12**
6. Annual Subscription Price: **$59.00**
7. Complete Mailing Address of Known Office of Publication (Not printer):
   Boland Hill Media LLC
   800 Roosevelt Road Building B Suite 212
   Glen Ellyn, IL 60137
   Contact Person: John Stewart Telephone: (877) 658-0418
8. Complete Mailing Address of Headquarters of General Business Office of Publisher (Not printer):
   Boland Hill Media LLC
   800 Roosevelt Road Building B Suite 212
   Glen Ellyn, IL 60137
9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor:
   Robert A. Jenisch
   Boland Hill Media LLC
   800 Roosevelt Road Building B Suite 212
   Glen Ellyn, IL 60137

   John Stewart
   Boland Hill Media LLC
   800 Roosevelt Road Building B Suite 212
   Glen Ellyn, IL 60137

   John Stewart
   Boland Hill Media LLC
   800 Roosevelt Road Building B Suite 212
   Glen Ellyn, IL 60137
10. Owner (If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.):
    Boland Hill Media, LLC **Same as block 7**
    Robert Jenisch **Same as block 7**
    John Stewart **Same as block 7**
11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities (if there are none, so state): **None**
12. Tax Status (For completion by nonprofit organizations authorized to mail at special rates): **Not applicable**
13. Publication Title: **Digital Transactions**
14. Issue Date for Circulation Data Below: **September 2019**
15. Extent and Nature of Circulation:

	Average number of copies of each issue during preceding 12 months	Number of copies of single issue published nearest to filing date
a. Total Number of Copies (Net press run)	23,136	23,541
b. Legitimate Paid and/or Requested Distribution (By Mail and Outside the Mail)		
1. Outside County Paid/Requested Mail Subscriptions Stated on Form PS Form 3541. (Include direct written request from recipient, telemarketing and Internet requests from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies)	13,052	13,481
2. In County Paid/Requested Mail Subscriptions stated on PS Form 3541. (Include direct written request from recipient, telemarketing and Internet requests from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies)	0	0
3. Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid or Requested Distribution outside USPS	0	0
4. Requested Copies Distributed by Other Mail Classes Through the USPS (e.g. First-Class Mail)	0	0
c. Total Paid and/or Requested Circulation [Sum of 15b (1), (2), (3), and (4)]	13,052	13,481
d. Nonrequested Distribution (By Mail and Outside the Mail)		
1. Outside County Nonrequested Copies Stated On PS Form 3541 (include Sample Copies, Requests Over 3 years old, Requests induced by a Premium, Bulk Sales and Requests including Association Requests, Names obtained from Business Directories, Lists, and other sources)	7,505	7,240
2. In County Nonrequested Copies Stated on PS Form 3541(include Sample Copies, Requests Over 3 years old, Requests induced by a Premium, Bulk Sales and Requests including Association Requests, Names obtained from Business Directories, Lists, and other sources)	0	0
3. Nonrequested Copies Distributed Through the USPS by Other Classes of Mail (e.g. First-Class Mail, Nonrequestor Copies Mailed in excess of 10% Limit mailed At Standard Mail or Package Services Rates)	0	0
4. Nonrequested Copies distributed Outside The Mail (Include Pickup Stands, Trade Shows, Showrooms and Other Sources)	2,161	1,969
e. Total Nonrequested Distribution (Sum of 15d (1), (2), and (3))	9,666	9,209
f. Total Distribution (Sum of 15c and e)	22,718	22,690
g. Copies not distributed	418	851
h. Total (Sum of 15f and g.)	23,136	23,541
i. Percent Paid and/or Requested Circulation (15c divided by f times 100)	57.5%	59.4%

16. Electronic Copy Circulation

a. Requested and Paid Electronic Copies	0	0
b. Total Requested and Paid Print Copies (15c) + Requested/Paid Electronic copies (16a)	13,052	13,481
c. Total Requested Copy distribution (15f) + Requested/Paid Electronic copies (16a)	22,718	22,690
d. Percent Paid and/or Requested Circulation (Both print & electronic copies) (16b divided By 16c x100)	57.5%	59.4%

X I certify that 50% of all my distributed copies (electronic and print) are legitimate requests or paid copies.

17. Publication of Statement Ownership for a Requester Publication is required and will be printed in the **November 2019** issue of this publication.
18. Signature and Title of Editor, Publisher, Business Manager or Owner:
    John Stewart, Editor Date: Oct. 9, 2019

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

EUROPE'S ALL-EMBRACING DATA REGULATIONS

Payments companies that handle consumer data in Europe are becoming quite familiar with the General Data Protection Regulation and the Secure Customer Authentication rules. Think you're immune because you're a U.S. company? Think again.

BY JIM DALY

IF YOU'RE ONE of the 500-million-plus consumers in the European Union, you might be proud that authorities last year implemented the General Data Protection Regulation, or GDPR, considered by many to be the world's strongest set of privacy protections.

You also might find further evidence that authorities are on the side of consumers regarding data-security matters now that the Strong Customer Authentication rules for online electronic payments officially took effect Sept. 14.

Never mind that so many merchants and other affected firms could not meet that deadline that pan-European authorities in effect declared an enforcement holiday and kicked the compliance can down to national governments.

SCA takes cues from private-industry security practices and rules already in force in the U.S. and elsewhere, including the newly updated 3-D Secure technology used for protecting online payment card transactions. Technically, SCA is part of an updated, broader regulation called the second Payment Services Directive, or PSD2.

Why should Americans care about these European regulations? In this online era of instant worldwide communications and global social networks and payment systems, what starts in Europe seems unlikely to stay in Europe. Here's what a spokesperson for fraud-prevention technology provider Riskified Ltd., which has offices in Tel Aviv, Israel, and New York City, says about PSD2/SCA in an email:

"The rollout of the regulation in Europe is being watched closely by the U.S. payments industry amid increasing fear that CNP [card-not-present] fraud will increase in America and other regions that don't have similarly strong protections. The U.S. is also widely predicted to adopt similarly strong protections, with adoption in the EU from companies like Amazon expected to speed the deployment here."

The GDPR, meanwhile, already has had a minor direct effect on Americans—credit, or blame, the regulation for those Internet pop-ups telling you a site uses cookies. The GDPR, which succeeded an older regulation called Data Protection Directive, sets up a whole troupe of actors on the privacy stage who are entrusted with protecting data, and that includes payments companies and social networks.

Its proscriptions could serve as models for lawmakers and regulators in the U.S. and elsewhere trying to address growing fears about eroding consumer privacy. "Regulators are certainly watching it with interest," says Zilvinas Bareisis, a London-based senior analyst who follows payments issues for the U.S. research and consulting firm Celent, a unit of New York City-based Oliver Wyman.

Adds Eric Grover, a payments consultant with Minden, Nev.-based Intrepid Ventures who has worked on international projects: "The short answer is anybody that transacts, wants to do business, is going to be affected."

'THE INDUSTRY IS STRUGGLING'

What follows is a high-level summary of the PSD2/SCA and GDPR, with a promise to keep the bureaucratese to a minimum.

The basic tenets of SCA, whose scope includes bank withdrawals and card payments, are familiar to just about any U.S. merchant or payment executive concerned with online security. SCA requires authentication to use at least two of three elements, according to a backgrounder from Stripe Inc., a San Francisco-based merchant processor with international operations.

These are: something the customer knows, such as a password or PIN; something the customer has, such as a smart phone, dongle, or other hardware token; and something the customer is, which may include a biometric such as a fingerprint or facial-recognition image.

These requirements apply to customer-initiated online payments within the 31 countries of the European Economic Area, a single market that includes the European Union's 28 members and three others. Stripe expects SCA to be enforced in the United Kingdom even if that country finally goes through with its long-planned but politically excruciating exit from the EU.

So what counts as strong customer authentication? The payment card networks' 3-D Secure version 2 does. EMVCo, the card-network-owned standards body, recently updated 3-D Secure, with one major goal: to make the customer checkout experience smoother as well as more secure. That had been a sore point for online merchants who complained buyers had to leave their Web sites during the checkout process under 3-D Secure's earlier iteration, leading to lost sales.

Also passing the test, according to Stripe, are the built-in biometric or password-based authentication flows in some mobile-payment systems, including Apple Pay and Google Pay. Stripe also said it expects several local European payment services will follow the SCA rules without major changes to the user experience.

But some authentication protocols fail the SCA test. One of the most prominent is the one-time passcode delivered to devices by SMS, the technology behind text messages.

Not every online payment requires SCA. Depending on the size of the transaction, exemptions are possible if the payment provider or bank's overall fraud rates are below set thresholds. Exemptions also are available in other scenarios, including certain merchant-initiated transactions using card-on-file data.

What happens if a merchant, or by extension its processor, doesn't follow the SCA requirements? The bank or other card issuer is supposed to reject the authorization request.

But this summer, with the Sept. 14 deadline looming, the card industry was a long way from being ready, according to a July Celent report written by Bareisis.

"According to research by (British bank and finance-company association) UK Finance, 25-30% of e-commerce card transactions would become impossible to complete as things stand," the report says.

Bareisis says that although the SCA's requirements officially took effect Sept. 14, European Union regulators "acknowledged the industry is struggling, so they allowed national regulators to put in their own plans on how to become compliant."

UK Finance is devising such a compliance plan for Britain, and authorities in other major European countries are doing so for their jurisdictions, according to Bareisis.

GDPR'S VAST SCOPE

Similarly, the GDPR contains a vast amount of details. But a critical reason why U.S. payments firms need to become acquainted with it is that its scope applies not just to European companies, but to companies anywhere in the world that in some way process European consumers' data.

'GDPR is seen as a solution to curb [privacy] issues.'

—ZILVINAS BAREISIS, SENIOR ANALYST, CELENT

A number of leading U.S. merchant processors have sizable European operations. They include: Fiserv Inc., which recently acquired First Data Corp.; Fidelity National Information Services Inc. (FIS), the new owner of Worldpay Inc.; and Global Payments Inc., which recently acquired Total System Services Inc. (TSYS). A smaller one is Atlanta-based acquirer EVO Payments Inc., which generates the majority of its transactions in Europe.

The GDPR defines personal data broadly, according to a separate Stripe analysis. "Personal data is not just a person's name or email address. It can also encompass information such as financial information or even, in some cases, an IP [Internet Protocol] address," the analysis says.

The 119-page regulation defines and spells out the duties of "data controllers" and "data processors." We'll spare you the details here. Suffice to say processing entities must meet a host of conditions, including that the subject of the data has given consent for its use, that the data processing is necessary for the performance of a contract, and several others.

The GDPR also is famous for its provision expanding its predecessor regulation's right for consumers to demand erasure of their data—the so-called right to be forgotten.

Violations of GDPR rules can carry severe fines—up to 4% of global revenues or €20 million ($22.1 million), whichever is higher. A British agency enforcing the GDPR in the United Kingdom this summer hit British Airways and the Marriott hotel chain with proposed fines of $230 million and $123 million, respectively, after the companies experienced big data breaches. Both firms indicated they would appeal, according to CNBC.

Some of the U.S. processors with European operations did not respond to *Digital Transactions'* requests for comment for this story. But a spokesperson for EVO Payments says the company has rolled GDPR compliance into its operations.

"We implemented a lot of those changes a couple of years ago … we're fully compliant with that," the spokesperson says in an email.

Some of the data-protection issues the GDPR tries to address actually originated with incidents not in Europe but in the United States, according to Celent's Bareisis, including the massive 2017 data breach at credit-reporting agency Equifax Inc. that compromised 148 million files.

"A lot of these issues bubbled to the top," he says. "I think GDPR is seen as a solution to curb these issues."

Clearly, non-European processors will need to familiarize themselves fully with the GDPR and PSD2/SCA if they want to pursue Europe's electronic-payments market. Processors also should get ready for what's next, says consultant Grover.

"This is no surprise, they're going to have PSD3," he says. "It's already percolating. You can take that to the bank." DT

TAP-AND-PAY'S EXPRESS TRAIN

After years of looking to make fare payment easier, mass-transit agencies have found the answer in contactless cards. That's giving consumers a compelling reason to use contactless on a broader scale.

BY **PETER LUCAS**

MASS ADOPTION of a new technology requires giving consumers a compelling reason to use it on a daily basis. Contactless cards are no exception.

For years, financial institutions needed merchants to install contactless terminals before they would issue contactless cards en masse. But merchants wanted the cards in circulation before investing in the terminals. The result: Contactless payments languished.

Enter that compelling reason for consumer use. Contactless barriers are breaking down as mass-transit agencies around the country roll out open-loop fare systems, a move that promises to give riders a reason to use contactless every day and could have spillover effects as these same users start interacting with contactless terminals at stores.

Momentum for mass transit's adoption of open-loop systems got a huge boost earlier this year as New York City's Metropolitan Transportation Authority (MTA) and the Miami-Dade County Department of Transportation and Public Works (DTPW) began accepting general-purpose contactless cards for fare payment.

By contrast, closed-loop contactless systems, which many transit agencies in the U.S. have introduced or plan to, allow consumers to preload value on to a contactless card, but that card can only be used to pay for transit fares. They're not interoperable with other networks.

The rollouts in New York and Miami are being closely watched because the MTA and DTPW operate in two of the 10 most populous metropolitan areas in the United States. That means they can collectively introduce contactless technology to millions of consumers and get them into the habit of using the technology multiple times daily just for transit.

In 2018, weekday subway ridership in New York averaged more than 5.4 million, and average weekday ridership for the MTA's bus system exceeded 1.8 million. The Miami Dade DTPW system has about 6.7 million bus and train riders per month.

Now, payments experts figure the habit of everyday transit use will make consumers comfortable with tap-and-go payments for all sorts of everyday purchases. That's why issuers and the card networks were eager to have as many contactless cards in consumers' hands as possible prior to the MTA's launch, payment executives say.

JPMorgan Chase & Co., which began issuing contactless cards at the start of the year, had issued about 20 million contactless cards as of May. One reason for banking giant's push was to ensure cardholders in New York could use their Chase cards to ride the MTA.

"One trend we are seeing in other cities where transit agencies have rolled out open-loop contactless systems is that consumers actively use their contactless cards for purchases at merchants near transit stations," says Linda Kirkpatrick, executive vice president for U.S. merchants and acceptance at Mastercard Inc. "In some of those merchant locations, we are seeing double-digit lifts."

'IMPORTANT USE CASE'

In all, 20 cities in the United States have either rolled out open-loop contactless systems for commuter-fare payment or plan to. Cities where contactless-fare systems have been introduced include Chicago and Portland, Ore., where the Chicago Transit Authority and Tri-Met Transit Authority, respectively, accept contactless payments for bus and train fares.

(Photo: Visa)

Can daily mass-transit use train consumers to use contactless cards—and mobile wallets—at the point of sale?

Transit agencies in Boston, Los Angeles, San Francisco, and Washington D.C. are reportedly planning to introduce open-loop contactless-card or mobile-based payment systems. Mobile-based systems typically include a tap-and-go feature, making them perfect for quickly moving commuters through a turnstile.

So far, adoption rates by consumers where open-loop contactless systems have rolled out have been impressive. The MTA reached 1 million taps in August after launching May 31. The volume was three to four times more than projected, according to the MTA.

Similarly, the regional transit authority TransLink in Vancouver, where contactless acceptance for transit launched in May, logged 1 million fares paid with contactless cards in two months. The biggest success story in mass transit, however, is in London. More than four years after launch, 50% of all Tube (subway) and train riders pay with a contactless card or mobile device.

Driving consumer acceptance of contactless for mass transit is the speed, security, and convenience of tapping to pay in an on-the-go environment, says Dan Sanford, global head of contactless payment for Visa Inc. Then, once introduced to the benefits of paying for transit fares with contactless cards, consumers are more apt to pay for purchases elsewhere using the same cards or mobile wallets.

"Transit continues to be an important use case for introducing consumers to tapping to pay as riding public transportation to and from work, home, or school is a critical part of daily life," Sanford says. "Tapping to ride helps introduce contactless payments to more consumers and can have a positive impact on the way consumers pay for things every day, even beyond transit."

Outside the U.S., Visa says more than 50% of consumer face-to-face transactions through its network occur with a tap, as opposed to inserting a card in a point-of-sale terminal. That's up from less than 30% two years ago. In addition, contactless payments represent at least one-third of all face-to-face transactions in nearly 50 countries, up from 35 countries at the end of Visa's last fiscal year.

Helping to accelerate mass transit's adoption of open-loop contactless systems is the increasing number of cards coming into circulation in the United States. Visa expects 100 million Visa-branded contactless cards to be issued this year and 300 million cards to be in circulation by year-end 2020.

Mastercard says it has commitments from issuers to bring more than two-thirds of its volume to contactless cards in the U.S. over the next two years. As of July, American Express Co. has publicly stated all new and replacement cards will be contactless.

Meanwhile, merchants are ramping up their ability to accept contactless cards. Mastercard says nearly 60% of its U.S. card-present volume originates at contactless-enabled merchants. Visa says 82 of its 100 largest merchants by transactions in the U.S. offer tap-to-pay at checkout.

That figure, which does not mean all transactions are contactless, is higher in such categories as grocery and drug stores, quick-service restaurants, and transit, where speed and convenience are valued by consumers, Visa says.

OPEN TO OPEN-LOOP

Now that the chicken-egg conundrum facing contactless cards is being addressed, transit agencies that previously launched proprietary contactless fare systems, such as Dallas Area Rapid Transit (DART), are moving to open-loop systems.

"When we first began looking at contactless acceptance in 2011, [general-purpose] contactless cards were not widely distributed, so it did not make sense for us to go that route," says Tina March-Pierre, assistant vice president for innovation at DART.

Now DART, which began rolling out its proprietary system in 2015, plans to start piloting open-loop acceptance in the December-January period, and begin a rollout some time in the first quarter of 2020.

March-Pierre cautions, however, that the rollout is dependent on how smoothly the pilot goes and whether there are enough contactless-card holders in its

Source: Visa

operating area to justify the move. To determine the latter, DART is talking to issuers in the region about their contactless card plans.

Other transit agencies that were early adopters of proprietary contactless fare systems include Chicago's CTA, which has since added open-loop acceptance.

Transit agencies are also starting to think beyond single-fare transactions. Now, they are looking to broaden use of contactless technology to include the purchase and use of daily, weekly, and monthly passes that can be stored in a mobile wallet or tied to a contactless credit or debit card.

For many transit agencies, the first step in this process is fare-capping. That's a practice in which a rider paying for one-way fares throughout the day makes enough trips to equal the amount of a daily pass. Once the cost of a daily pass is reached, the cardholder is no longer charged for rides that day.

"Fare-capping is something a lot of transit agencies do and is relatively easy to implement," says Juan Ortiz, regional director, business development, for Bytemark Inc., a New York City-based provider of transit-fare solutions, including contactless acceptance. "One reason transit agencies are deploying open-loop systems is their versatility when it comes to adding modules to support other fare options."

The Miami-Dade DTPW, which launched its open-loop system in August at 23 commuter-train stations with plans to add bus fares in the following weeks, supports daily fare-capping for consumers paying with contactless cards.

Looking ahead, the agency plans to add digital monthly passes that can be downloaded to a mobile wallet. The Miami-Dade DTPW accepts contactless bank cards, digital wallets such as Apple Pay, Google Pay, and Samsung Pay, and wearable devices such as Fitbit.

But supporting daily and monthly passes through its contactless-fare system is just the tip of the iceberg. The Miami-Dade DTPW also plans to create regional passes that are interoperable with transit agencies in adjacent Palm Beach and Broward counties as well as with third-party transit providers, such as Uber and Lyft.

By purchasing a regional pass that can be loaded into a mobile wallet, a commuter can enjoy unlimited rides on any mode of transportation within the boundaries of the pass and for the duration of the pass.

For example, a commuter who has purchased a monthly regional pass can take an Uber from his apartment to a train station, then board a train to the airport—or have the cost of the trip covered as part of the fee for the pass.

"Having one app that works across all modes of transportation brings economies of scale to fares for consumers by eliminating multiple fare schedules, and allows the commuter to pay with a single option," says Alice Bravo, director of Miami-Dade DTPW.

One reason Miami-Dade DTPW is moving to support monthly passes and regional fare cards that can be loaded into mobile wallets is so consumers don't have to check their credit card statement to see if they have been properly charged for each fare, Bravo says.

BULLISH ON THE FUTURE

As more transit agencies embrace open-loop contactless cards and issuers put cards in the hands of consumers, payments experts are bullish about the future of broader contactless-card acceptance in the United States.

"Mass transit is helping to build out the contactless infrastructure in the U.S.," says Matt Cole, president of San Diego-based Cubic Transportation Systems, which has worked with Visa and Mastercard and several transit authorities to install contactless systems. "And that helps usage in the retail world take off." DT

Ever-rising fraud doesn't have to be inevitable.

endpoint

FRAUD CONTROL: GOOD NEWS, BAD NEWS

On the one hand, fraud losses continue a seemingly inexorable rise. On the other, there are positive steps businesses can take to mitigate those losses.

BY **JIM WRIGHT**

Jim Wright is vice president, enterprise sales, at Nvoicepay Inc., Beaverton, Ore.

EARLIER THIS YEAR, the AFP (the Association for Financial Professionals) published its annual "Payments Fraud and Control Survey," which looks at trends in business-payments fraud and what companies are doing to combat them.

The news wasn't particularly good. Even though companies are finding some success with increased fraud-prevention efforts, they're having trouble keeping pace. Eighty-two percent of the survey's 628 respondents said their organizations experienced attempted or actual payments fraud in 2018. That represents a nearly 20% rise in the past five years. We're at a point where it's no longer a question of whether your business will experience fraud, but when.

What stands out in this year's report is that criminals keep finding new ways to attack businesses, and they're increasingly attacking large enterprises. No company is immune, and businesses need to find even better ways to safeguard every type of payment along with the payment process itself, because the fraudsters are always one step ahead.

Business email compromise (BEC) is a top tactic for external attacks, impacting more than half of the survey respondents, up from 46% in 2017. Wire transfers are still the most common target for BEC scams, probably because they're usually one-off requests, so it's less noticeable when something is out of the ordinary. Checks are the second most common target because they're still the most common payment method.

The good news is that, with heightened awareness and defenses, the number of companies experiencing BEC wire payments fraud has dropped 17 percentage points, from 60% to 43%.

The number of companies hit by BEC fraud targeting checks has dropped as well. Nearly 90% of organizations now report using Positive Pay. Roughly 70% say they have instituted internal controls such as segregation of accounts and daily reconciliation to fight check fraud. These measures appear to be working. Just 20% of companies reporting BEC scams said they targeted paper checks, a 14-point decline from the previous year. That far outpaces the decline in use of paper checks, which remains stubbornly stuck at about 50%.

The bad news is that one-third of companies reporting said fraudsters accessed automated clearing house credits via BEC, up from

12% in 2017 ("A Surprising Jump in ACH Fraud," May). According to the report, that means that criminals are now more able to invade internal systems through account takeovers (ATOs), and access harder-to-reach payment methods. This has caught companies off guard: 56% of survey participants said they aren't taking any additional steps to protect ACH payments.

Another ominous trend: Although monetary losses haven't increased much per company (scams are typically designed to evade red flags by requesting ordinary amounts of money), fraudsters have stepped up attacks on large enterprises where bigger payments are more common. And they're stealing larger amounts of money. Twenty-five percent of companies with over $1 billion in revenue and 100 or more payment accounts reported losses of $1 million or more from BEC.

A MULTIFRONT BATTLE

What can companies do to protect themselves? They must fight this battle on many fronts. They should set up training, protocols, and controls to address different schemes, payment methods, and associated processes.

> 'Payment fraud has become a game of whack-a-mole that the moles are winning.'

Education, training, and internal controls that prohibit payment initiation based on emails or other secure messaging systems are the top means to guard against BECs. Verification policies and minimum two-factor authentication are both important, too, because scams are getting more and more convincing.

Positive Pay is a good first step against check fraud. You can take it a step further with Payee Positive Check, which adds the payee name to the data fields that are cross-checked.

Companies that actively protect themselves against ACH fraud use a variety of measures, including:

- Reconciling accounts daily to identify and return unauthorized debits;
- Blocking all ACH debits except on a single account set up with ACH Positive Pay and a debit filter;
- Blocking ACH debits on all accounts, and creating a separate account for ACH debits initiated by third parties, such as taxing authorities.

Daily reconciliations are also a common way of protecting against attacks on security credentials. Other protections include: restricting access to company networks to company-issued devices; dedicating to payment origination a personal computer with no access to email, web browsers, or social networks; and instituting disaster-recovery plans.

On the card-payment side, single-use virtual cards are the most secure way to pay invoices, because the card number can only be used once, and only for a specified amount and payee. If all that sounds like a lot of work, consider automating payments through a third-party platform.

Payment fraud has become a game of whack-a-mole that the moles are winning. Companies have battened down the hatches on some fronts, only to find fraudsters popping up elsewhere. Despite some success in the battle, overall fraud continues to rise.

Companies should consider every means at their disposal to protect not only the payments themselves but the associated information, systems, and processes. DT