DIGITAL®
TRANSACTIONS

Trends in the Electronic Exchange of Value

THE
BANKS
STRIKE
BACK

THEY'VE LANDED WITH FORCE IN THE P2P MARKET. HOW ARE FINTECHS LIKE VENMO AND SQUARE REACTING?

ALSO IN THIS ISSUE

hello future.

Tomorrow's payment possibilities today.

TSYS® has harnessed the power of payments so you can help businesses achieve their full potential in today's ever-changing world. Through continuous innovation and our comprehensive suite of solutions, the possibilities are endless.

UNIFIED COMMERCE · INTEGRATED POS · PAYMENTS · PREPAID CARDS

TSYS®

Call 866.969.3350

Introducing Harbortouch Checkout™

Retail POS that's easy to use and easy to sell

Build the ultimate portfolio with POS

Harbortouch has pioneered POS within the payments industry and has become the leading POS provider for the hospitality market. Now, we are thrilled to introduce a powerful and easy-to-use retail offering that delivers a massive new opportunity for our sales partners. Harbortouch Checkout hits the sweet spot for the vast majority of retail merchants, delivering all the features they need in an intuitive and user-friendly software package. Its easy-to-use design makes it easy to sell. And, of course, it will be offered as part of our unparalleled free POS program so it can't be beat on price!

Why Sell Checkout?

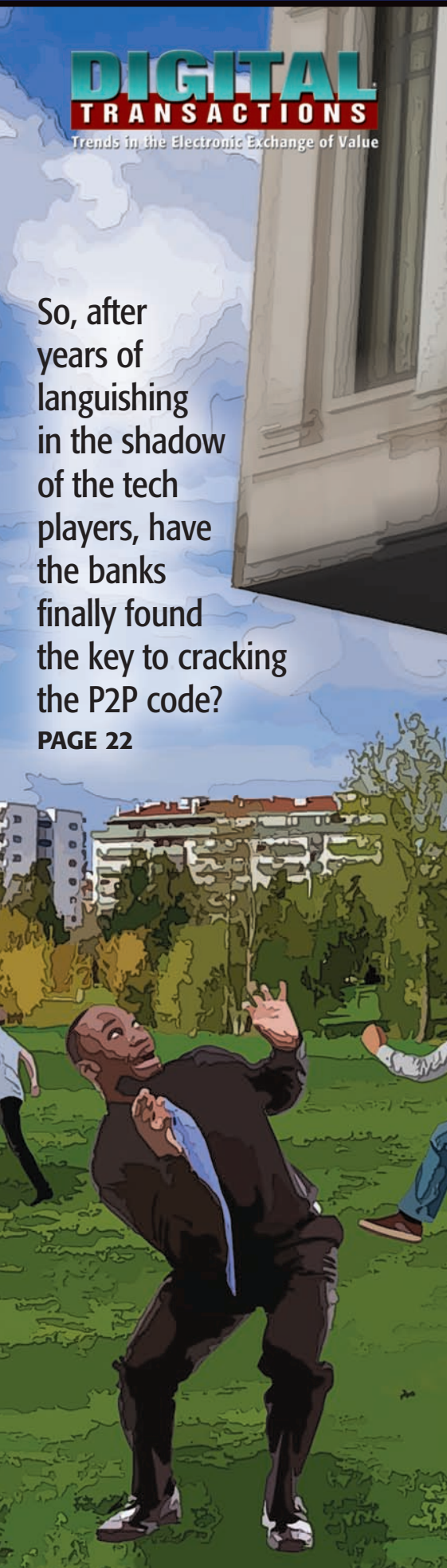| Easy to use software makes it easy to sell | POS delivers high volume accounts with low attrition | Powerful software is feature-rich, yet simple and intuitive | Built-for-purpose equipment with a lifetime warranty | Remote reporting, POS management and inventory tracking |

Learn more about Harbortouch POS at www.isoprogram.com

Brian Fitzgerald, National Sales Manager Central - 800-201-0461 x 1257 or bfitzgerald@harbortouch.com
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

HARBORTOUCH®
A SHIFT4 COMPANY

DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

So, after years of languishing in the shadow of the tech players, have the banks finally found the key to cracking the P2P code?
PAGE 22

CONTENTS

June 2018 ■ Volume 15, Number 6

Cover illustration: Jason Smith, Fotolia.com

THE GIMLET EYE

P2P's Newtonian Reaction

Call it Newtonian market dynamics. Sir Isaac Newton propounded the physical law that for every action there is an equal and opposite reaction. Now, in the suddenly vibrant market for person-to-person payments, we're seeing an analogous reaction unfold. As our cover story on page 22 explains, financial institutions have made a strong comeback in P2P with their Zelle network. That's a reaction opposite to the serious inroads made by nonbank providers such as Apple, Square, and, most prominently, Venmo.

Opposite, but is it equal? In some ways, "comeback" may be not quite right. Financial institutions were already processing large volumes of P2P transactions even before Zelle debuted last summer. They were doing it through systems like Popmoney, People Pay, and the Zelle forerunner clearXchange. They just weren't getting much notice for it. Instead, the publicity went to systems like Venmo that catered to 20- and 30-somethings with a clever twist: social media. Not only can you pay a friend, landlord, or relative, you can let them—and all your friends—know about it in the Venmo feed.

Zelle's average ticket is higher than that of Venmo, indicating it's dealing with more than just split payments for dinners out, baby sitters, and theater tickets. Perhaps it's seeing a bigger influx of rent payments or other quasi-commercial transactions. That profile should flatten out as more users adopt it for ordinary payments to friends and family.

What Zelle and its rivals will have to figure out is how to make some money on these services, all of which are offered free of charge to the user. It's no good saying P2P doesn't have to make money, that it can simply drive business to unrelated financial services that carry lucrative fees. There's too much expense involved in building and maintaining a network, and volume-driven network economics will only get you so far.

Companies like PayPal, which owns Venmo, already see this. That's why it's pushing Venmo into retail stores—more than 2 million of them so far—in a program called Pay With Venmo. Payments are still free to users, but PayPal earns a merchant fee on each transaction.

Even Zelle is acting on this front. It's beginning to process disbursements—things like payouts from insurance companies to policyholders—on its real-time network. Those fast payouts please customers and earn a fee for the participating bank, though Early Warning, the bank-owned company that runs Zelle, won't disclose it at this early date.

Once the economics of P2P are sorted out, the market will really boom. Meanwhile, the bank vs. nonbank battle, played out in so many other arenas over the years, plays on in this one.

John Stewart, Editor | john@digitaltransactions.net

Smart Retail Solutions

Introducing PAX's new Smart Retail Solutions. Sleek designs that make them look more like a tablet than a payment terminal.

PAXSTORE

PAX has launched an application management platform for resellers and partners to manage applications with the PAX Smart Retail Solutions.

US Headquarters:
4901 Belfort Road, Suite 130
Jacksonville, FL 32256
+1-877-859-0099 | sales@pax.us

Regional Office:
40 West Baseline Road, Suite 210
Tempe, AZ 85283
+1-877-859-0099 | sales@pax.us
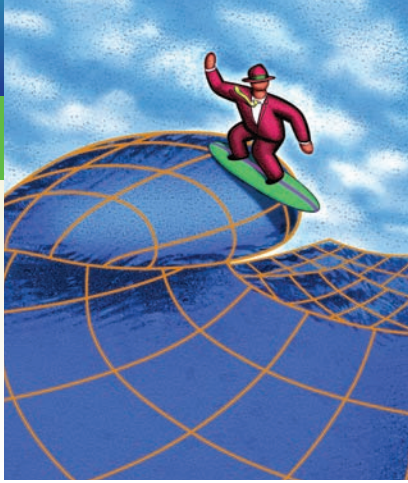
Rerouting Payments Around the Card Networks

First it was retailers, which tried but failed. Now an airline trade group wants to develop a payment system that would bypass the credit card networks, theoretically saving carriers billions in interchange.

The proposal comes from the International Air Transport Association, which says it has 280 members representing 83% of air traffic. The group lists its headquarters as Montreal but has executive offices in Geneva, Switzerland.

The IATA's payment project, which involves Germany's Deutsche Bank, was first reported in May by London's *Financial Times*. The system is designed for the European market, at least at first. The project is possible because under the new Payment Services Directive 2 regulation taking effect in the European Union, third parties will be able to access certain bank-customer data and be able to initiate payments themselves.

According to the *FT*, a user would enter his bank-account data, and Deutsche Bank would verify whether sufficient funds were available, then move the funds out of the account to the airline.

A payment transaction would cost the airline "a matter of cents," an IATA executive quoted by the newspaper said. In contrast, airlines typically pay 1% to 3% of fares for card-acceptance costs, adding up to $8 billion a year, IATA estimated.

An IATA spokesperson tells *Digital Transactions* by email that the project should be ready for testing by year's end.

"The purpose of this pilot is to develop and test a payment option on

Can the IATA airlines and Deutsche Bank divert transactions from the major card networks?

Web sites of airlines participating in the pilot project, using the capabilities of real-time or near real-time direct bank transfer," the spokesperson says.

"Similar payment methods are already offered by some airlines around the world, but each is a proprietary solution, whereas the IATA-Deutsche Bank pilot will test a solution that is applicable to all airlines' transactions specifically covered under PSD2," the spokesperson continues.

The spokesperson adds that for airlines, direct payment could "offer a cost-competitive solution, while avoiding the losses associated with fraudulent credit card transactions. For air travelers, it would represent a fully secure additional payment option."

The IATA proposal bears some similarities to the now-defunct Merchant Customer Exchange (MCX) established by dozens of U.S. retailers in 2012. MCX's joint payment system was dubbed CurrentC, was primarily oriented toward mobile devices, and would have bypassed the card networks.

But some MCX members, including Walmart, seemed to put more effort into their own mobile-payment systems and loyalty programs. After years of planning and some limited tests, the retailers abandoned the effort and sold CurrentC's technology to JPMorgan Chase & Co. in 2017.

But some observers believe the IATA's plan could succeed. In addition to the groundwork laid for the proposed system by PSD2, the IATA also is benefiting from years of customer-authentication and risk-control techniques developed by the airlines in the Internet age, according to Richard K. Crone of San Carlos, Calif.-based Crone Consulting LLC. A key part of that is the increase in cards on file that the airlines have from customers.

"What makes this possible is a high degree of confidence" in getting a secure payment because "they have a known user," Crone says.

But another airline group that already operates a payment system, the Washington, D.C.-based UATP, is skeptical of the IATA plan because of Deutsche Bank's involvement, though a spokesperson says UATP is not yet fully informed about it.

"Since we are the airline industry's wholly-owned payment network, we expect to be involved in cost-reducing initiatives and would be wary that a commercial bank has the same interest," the spokesperson says by email.

—*Jim Daly*

As Synthetic ID Fraud Booms, Solutions Prove Elusive

Fraudsters are not just buying stuff with stolen consumer payment credentials. They're increasingly using information they glean from data breaches to invent fresh identities, sometimes out of whole cloth, leaving credit card issuers, banks, and other lenders holding the bag.

Indeed, the losses from so-called synthetic identity fraud are mounting fast. Card issuers alone sustained $820 million in synthetic ID fraud in 2017, up fully 41% in just two years, according to a new report from Aite Group LLC (chart). On current trends, the firm projects these losses will swell to more than $1.2 billion by the end of 2020.

"It really is a perfect storm," says Julie Conroy, research director at Boston-based Aite and the report's author. While growing fast, the problem at many organizations remains cloaked in misunderstanding and confusion, leading Aite to call it "the elephant in the room."

In fact, Conroy's report, "Synthetic Identity Fraud: The Elephant in the Room," shows loss data only for credit card issuers, even though synthetic ID fraud also plagues auto lenders and other credit grantors. That's because only card issuers have compiled hard data, Conroy says. But risk managers across the board are starting

The Real Pain of Synthetic ID Fraud
(U.S. credit card losses, in millions)

$580 — 2015
$701 — 2016
$820 — 2017
$968[1] — 2018
$1,133[1] — 2019
$1,257[1] — 2020

1. Projected   *Source: Aite Group*

to get a clearer picture and to collaborate on solutions.

"This is not a new problem, but it is serious enough that [security officials] are coming together," Conroy says. She contrasts this development with the state of affairs in 2011, when Aite conducted its last round of research on synthetic ID fraud. "That [cross-industry cooperation] wasn't happening then," she says.

A number of factors account for the mounting losses, but there's no question the rash of data breaches is fueling the trend. Since 2013, hackers have accessed more than 9.7 billion records online, according to data from the card-technology company Gemalto cited in the report.

Victims now include credit-reporting agencies themselves, with Equifax Inc. last year sustaining a breach that affected 147.4 million records.

With this pilfered information, criminals can mix and match bits of data to invent personas that can then apply for credit lines and take out cash that will never be repaid. And once these personas become files at the three major U.S. credit bureaus, it's very difficult to root them out, Conroy says. "The problem is fairly systemic," she says. "It's going to take some fairly systemic solutions to really put a dent in this."

Complicating the search for solutions is a decision the Social Security Administration made in 2011 to randomize Social Security Numbers. Where once these numbers were derived from date and region of birth, they are now simply randomly generated digits, depriving fraud fighters of "a valuable tool ... that [financial institutions] could use to check the validity of an SSN at the time of account onboarding," says the Aite report.

Criminals are taking advantage of this change. Where fraud officers expected 3.6% of all SSNs to be
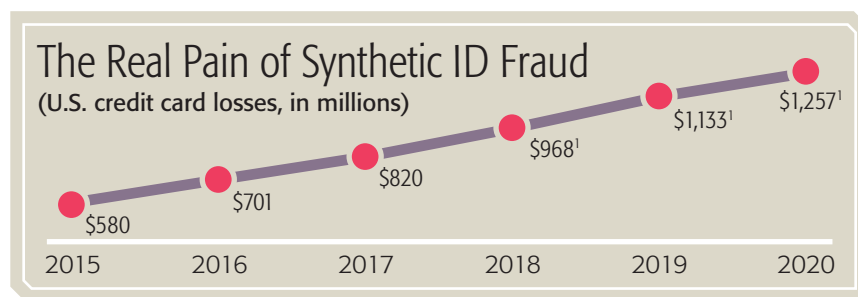
potentially randomized last year, the actual volume seen in credit applications was 5.8%, according to ID Analytics data cited by the report.

Ultimately, solutions will have to emerge to cut off the flow of data sooner, Conroy notes. "We need to have a way to detect synthetic records earlier so they don't get furnished to the credit bureaus in the first place," she says.

—John Stewart

How a Bank Zapped Zelle Fraud

Customers liked Zelle after PNC Bank last July rolled out the multi-bank person-to-person payments service, but so did fraudsters.

Paul Trozzo, senior vice president and product group manager, calls Zelle "very successful" for the Pittsburgh-based bank, a unit of The PNC Financial Services Group Inc. But Trozzo told attendees last month at the NACHA Payments 2018 conference in San Diego that "there absolutely were some growing pains."

Specifically, fraud for a time hit "double digits" in basis points of payment volume, Trozzo said at a panel session.

The high fraud rate prompted PNC to take several corrective measures, including: sending emails to Zelle customers to confirm a transaction was occurring on their account; making improvements in security for access to PNC accounts, especially through mobile devices; and working with mobile carriers to help thwart fraud.

Fraud now is running at a more "normalized" rate of 5 to 6 basis points (0.05% to 0.06%) of Zelle volume, according to Trozzo, though the bank continues to work on reducing it. PNC hasn't increased what Trozzo said is its conservative transaction limit of

$1,000, though he indicated the bank could re-examine that limit as Zelle's one-year anniversary comes up.

PNC customers are generating about 15,000 transactions a day on Zelle, and about 3,000 customers are signing up for the service daily. "It's continuing to grow as people start seeing value and benefits," Trozzo said. He also reported that PNC continues to offer Popmoney, the P2P service from processor Fiserv Inc. that the bank provided before rolling out Zelle.

Meanwhile, Zelle had "really good numbers for the first quarter," said another panelist, Laura Weinflash, vice president of product management at Early Warning Services LLC, the technology company that runs Zelle and is owned by some of the nation's biggest banks.

The service, which is now offered by many banks directly as well as smaller financial institutions through processor connections, posted 85 million transactions, up 14%, and is adding about 100,000 users per day, she said. (Read more about Zelle and the P2P payments market in "The Banks Strike Back," page 22).

Zelle, however, got a black eye in April when *The New York Times* reported that some users were getting hit with fraud for various reasons, including a lack of transaction notification in some cases and an apparent lack of vetting of recipients' identifiers such as phone numbers or email addresses, which Zelle uses to get money to their bank accounts. Zelle told the newspaper that fraud was under control and that there have been "very few" such incidents.

Payments analyst Aaron McPherson, vice president for research operations at Maynard, Mass.-based Mercator Advisory Group Inc., says the *Times'* story "was based more on anecdotal evidence than on real research."

Still, some banks' Zelle "implementations were rushed, without enough attention paid to making sure that alerts were in place," he says by email. And some customers incorrectly assumed that they were automatically covered by the zero-liability policies for fraudulent payment card transactions.

McPherson says Zelle's early fraud experience bears some similarity to that of Apple Pay after Apple Inc. rolled out the mobile-payment service in late 2014. Criminals discovered that they could load fraudulent cards into Apple Pay wallets, a problem Apple quickly corrected.

"I have no doubt that the [Zelle] problems will be fixed, and that the system is very safe overall; however, first impressions are difficult to overcome, and this will be a headwind on future growth," he says.

McPherson says banks should consider implementing some form of a fee-based guarantee that gives Zelle users protection when dealing with people they do not know well, "rather than simply complaining that they are using the service in the wrong way."

—Jim Daly

Apple's New Card Might Lock in Banks for Apple Pay

Apple Inc. appears to be creating a new Apple Pay credit card, with Goldman Sachs Group Inc. as the issuer. Whether the card will boost usage of the mobile-payments service is unclear, but one thing it seems likely to do is tighten Apple's links with thousands of banks that support the service.

The pending Goldman deal "really encourages those [financial institutions] that have already committed to Apple Pay to really promote it," notes Richard Crone, principal at Crone Consulting

LLC, a San Carlos, Calif.-based financial-services consultancy. The alternative is to lose customers to the Goldman-Apple Pay card while remaining obliged for the contractual period to support their own cards in the Apple Pay wallet.

The result could be improved consumer adoption and usage for Apple Pay, and enhanced revenue flows for Apple, which collects a 0.15% share of the transaction amount on each Apple Pay credit card transaction (half a penny on debit). Already, Apple Pay has attracted 40 million U.S. users that Crone Consulting considers "active," that is, making at least two transactions monthly.

By comparison, Google Pay and Samsung Pay, the wallet's two main tech-based rivals, have 15 million and 11 million active users, the firm estimates.

Still, while Apple Pay has opened a wide lead over these competitors, some observers have been puzzled by what they see as the company's shyness about promoting the wallet. A possible reason is that awareness levels are already higher for Apple Pay among consumers than any other wallet (chart).

Details of the Apple-Goldman tie-up are not yet known, as planning is apparently early and ongoing. The cobranded product is not expected to hit the market until early next year,

The Apple of the Consumer's Eye

(Awareness levels for select wallets, % of consumers surveyed)

Apple Pay	71%
PayPal Wallet	58%
Google Pay	44%
Samsung Pay	43%
Starbucks app	26%
Chase Pay	22%
Walmart Pay	21%
Capital One Wallet	16%
Dunkin' Donuts	12%
CVS Pay	6%
Kohl's Pay	6%

Source: Phoenix Marketing, data as of January 2018

according to *The Wall Street Journal,* which first reported the news.

But whether Apple Pay users stick with their existing cards or switch to the Goldman Apple Pay product, Apple stands to benefit. The computing giant could earn a 0.30% share of tickets under the Goldman deal, sources told the *Journal.* And it will collect a $100 bonus for each cardholder who signs up, those sources said.

Neither Apple nor Goldman responded to requests for comment from *Digital Transactions.*

Apple has turned to Goldman after

years of supporting a cobranded card with Barclays PLC. The new card, however, will carry branding specific to Apple Pay, which Apple launched in the fall of 2014 as a mobile wallet that depends on near-field communication for point-of-sale links and stores card credentials in a phone-based secure element. The Barclays card, too, features contactless as well as EMV capability.

The Barclays deal was due for rebidding, a process Goldman apparently won, according to Crone, who says Apple may well claim an even larger share of issuer interchange than the *Journal* report indicates. "I think it starts around two-thirds for Apple," he says. "If not two-thirds, then they will get a cut of the financing and other fees."

Meanwhile, financial institutions already supporting Apple Pay could face a stark choice: stick with the wallet, and possibly face higher revenue claims by Apple as its user base grows, or pull out and possibly lose cardholders to the new Apple Pay card. Crone figures they'll stay. "The exit costs are too high," he notes.

For Goldman, the new card could bolster the investment bank's relatively new thrust into consumer-based financial services that uses the brand name Marcus. **DT**

—*John Stewart*

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

Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017
2.435%	2.444%	2.490%	2.488%	2.468%
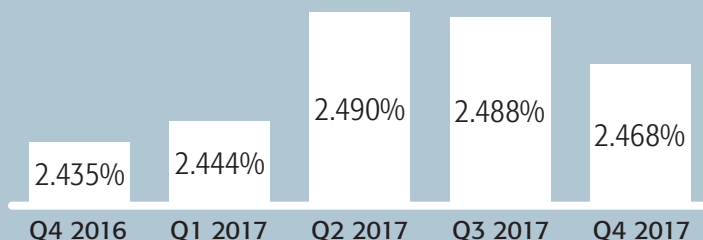
Note: This is sourced from The Strawhecker Group's merchant data warehouse of over 3 million merchants in the U.S. market. The ability to understand this data is important as small and medium-size businesses (SMBs) and the payments providers that serve them are key drivers of the economy.
All data are for SMB merchants defined as merchants with less than $5 million in annual card volume.

Security Notes

Payment in an AI Ecosystem

Gideon Samid • *Gideon@BitMint.com*

Payment should be efficient, secure, and convenient. Alas, these three objectives pull in different directions. Efficiency and convenience tend to undermine security; convenience pulls towards versatility, which in turn harms efficiency. A balance is called for, and the most daring ideas call for a dynamic rather than a static balance.

As payment migrated into cyber space, humanity found itself in a global financial village where everyone can pay and get paid by anyone else. Over 2 billion traders can send money to each other. The system can handle it. However, the reality is that each of us trades primarily with a small set of trading partners, and only rarely with an odd trader on the other side of cyberspace. We trade in clusters, and this fact is meaningful: Cluster-sharing traders experience mutual familiarity and mutual trust.

This fact can be exploited by leaning towards efficiency and convenience, scrubbing certain security burdens. The majority of our payments are in small denominations, where convenience and minimum attention are prime factors. Here, both efficiency and security are second-order priorities.

On the other end, we have few high-volume payments where security trumps both efficiency and convenience. This variance suggests a dynamic procedure.

A payer and a payee are about to execute a transaction. In today's reality, this transaction will be carried out according to some rigid protocol, whether this protocol is optimal or not. What we would rather have is a dynamic situation. In this situation, an intelligent agent would weigh a host of factors, like the amount of the transaction, its urgency; the attributes of the traders (merchants, shoppers, friends, investors), the relationship between the traders, the load on the various parts of the trading systems, and so on. Considering all these factors, this intelligent agent would map out a payment protocol tailored for this transaction, an optimized approach. The parties would be prompted accordingly.

Upon a deeper examination, it becomes clear that security is the culprit that accounts for payment complexity in cyberspace.

Consider for a moment a trading reality in heaven, where all traders are honest and trustworthy. One could then request that all traders simply keep a log of all the money they committed and all the money they are owed over some period of time, say a week. By the end of this week, all those who logged a net payout would pass this sum to a common cash register, and all those who logged a net in-flow would invoice the cash register with that amount. The cash register would distribute the money with perfect reconciliation. After all, it's heaven.

What is instructive about this depiction is the fact that no pay-as-you-go activity takes place. Instead, the sums are reconciled once every so often. This means that pay-as-you-go is the fastest possible flow—as fast as the time it takes to log the transaction—without the friction of actually moving money.

We may take this model as a reference, and define "heaven islands"—payment ecosystems where traders may be mutually regarded as perfectly honest. This happens upon intimate mutual familiarity, and upon enough reserves and mutual dependence, such that any fraud or dishonesty can be readily rectified. Such heaven islands would allow for a simple passing of digital money strings, with no security and no verification or elaboration.

Now imagine the full-scale ecosystem as a mosaic of such heaven islands accounting for the majority of the traders' activity—only that the described trading clusters are inherently dynamic. People move to a different state, and thereby change the cluster of people who pay them and to whom they pay. People change lifestyle, grow up, get old, and so on. The clusters of payments will be dynamically defined, and people will move between them like phone users pass between cell phone towers.

The actual payment algorithms will be dynamic as well. The main asset of cyber fraudsters today is the stability and standardization of today's payment procedures. They last long enough for fraudsters to engineer a way to crack them. But let these procedures undergo dynamic change, and they become a fast-moving target that is hard to crack. Even once cracked, the triumph is useful for only a short time.

Artificial Intelligence is the technology that can deliver this dynamic optimization of efficiency, security, and convenience. This is the promising future, which my company BitMint, like other digital-money creators, is planning for. ∎

Retail NOW 2018

AUG. 5-8
Nashville ★ TN

RSPA

- Protect your Merchants and your Business... Avoid the Next Breach
- Gain Insight on Market Basics & Salesperson Onboarding
- Expand your Portfolio and Pave the Way for Your Future
- Expand or Launch your Distribution Channel
- Establish New and Valuable Relationships
- Extend your Service Reach with Partnerships
- Learn and Grow from a Powerful & Unique "Team IQ"
- Refine Sales, Service Delivery, Recurring Revenue & Cashflow

A COMMUNITY EMBRACING OPPORTUNITY

REGISTER NOW!

www.GoRSPA.org/RetailNOW

GAYLORD OPRYLAND®
RESORT & CONVENTION CENTER
Nashville

Payments in the Time of Facebook

George Warfel • *GWarfel@haddonhillgroup.com*

Many years ago, in a press interview, I commented on the importance to banks and payment companies of understanding the then new phenomenon of Facebook. At the time, it looked as if social media might become a major platform for payments.

It turns out that mobile media has taken that role, and social media instead has offered a different lesson: without trust, all the new technology in the world is not going to matter.

Facebook will survive the crisis it has created by not being transparent about its business model. But payments processors could be more vulnerable to their customers abandoning them if they misuse the customer information they hold. Facebook's users have nowhere else to turn. But it's pretty easy for a bank's customers to find someone else to process their payments.

How much information about customers might a bank's marketing department desire to "scrape" if regulations or strong bank-privacy policies didn't prohibit it? It's one thing to try to sell customers banking services they might not need. It's quite another to sell their personal information to the highest bidder without their knowledge.

Might it be that in blithely adopting every new technology or platform that pops up (Bitcoin, anyone?), the banking industry is going to find out there is much more to be lost than gained? It might be prudent to do a little more testing of what happens out at the edges of the normal distribution curve when you turn over the management of a customer's payments entirely to a machine. As has been said, the problem with "lights out" data centers is that you can't see what's going on in there.

The disruptors are all agog about how artificial intelligence can deduce things about my payments that I may not even know. Is that alone sufficient reason to retire the guy in the wire-room who looks over my outgoing transaction for suspicious words or numbers and then holds the transaction up until he's sure it's both legitimate and safe, replacing him with an algorithm that wouldn't notice the subtle discrepancies? There is a world of difference between doing transactions the cheapest and fastest way and doing them the safest, if slightly costlier, way. It's a difference our customers might think worth the cost.

Which gets us back to the matter of value. Given the choice between a 100% automated way of approving and processing a transaction and inserting a knowledgeable person into the process, the latter is always going to cost a bit more and be a little bit slower. In such a situation, I hope I would find myself choosing the method that both the bank and our customer could trust the most, instead of whatever method promised a side benefit of generating new marketing information to sell customers things they hadn't asked for and possibly don't need.

The champions of moving fast and breaking things seem oblivious to what good bankers have always known: You are never going to gain enough by scraping and harvesting your customer's personal data to make up for the loss of their trust when they find out what you've been doing with the information they entrusted to you.

Most people probably wouldn't mind having their retina scanned to approve a transaction. But most are almost sure to object if they find out their bank was then going to sell their retinal pattern to the highest bidder. Then those patterns could be used to identify customers in photos plucked off the Internet to learn what kind of restaurants they habitually go to so the bank can target-market credit card offers to them. Or what type of sports events they attend so the bank can start marketing them seat-license loans.

What the 30-something billionaires don't get—that privacy matters to a lot of folks—is something we in the banking and payments business need to not only be sure we do get, but also be sure that we remember.

The adoption of new technology has propelled the payments business to its current levels of volume and profit. Perhaps the lesson of Facebook's comeuppance is that a new technology can be a speeding train in the night. Just blithely jumping on board could be dangerous. Or possibly fatal. ■

MPC
MOBILE PAYMENTS CONFERENCE

CUSTOMER ENGAGEMENT - MOBILIZING YOUR BUSINESS
August 22 - 24, 2018
Wyndham Grand Chicago Riverfront

To be the global intersection of Fintech industry experts and analysts - where connections are built to bring clarity to the world of mobile technology and payments

MOBILE PAYMENTS CONFERENCE: THE ONE EVENT YOU WON'T WANT TO MISS!

The Mobile Payments Conference is more than mobile payments, it is an invitation into a growing elite group of professionals who are holding a conversation that never ends. MPC will be held at the Wyndham Grand Chicago Riverfront, Chicago, IL, August 22 – August 24, 2018.MPC is this year's must attend event!

MPC Keynotes

Don Bush — Kount

Jack Connors — Google

Matt Donnelly — FREEDOM.PAY

Aaron Lint — ARXAN

Usha Nandigala — General Motors

MPC Confirmed Speakers

Jim Ciortan	Ed O'Neil	Jack Philbin	Michael Thelander
Cullen Talley	Jason Oxman	John Firman	FrankKerr
Jennifer Williams	Robert Mau	Larry Brennan	Sam Hall
Kassi Quimby	Michelle Tinsley	Thad Peterson	Travis Dulaney

Visit our website to see the full agenda: MobilePaymentConference.com

EXHIBITORS, SPONSORS, AND PARTICIPATING COMPANIES

451 Research · Aite · AD Technology · ARXAN Application Protection · aws · Bank of America Merchant Services · cardlytics · EPSON EXCEED YOUR VISION · eta · FINTEX · First Analysis

GRUBHUB · IBM · JAVELIN · Kount · MM&T MOBILE MARKETING AND TECHNOLOGY · NorthAmerican BANCARD · parallel communications group, inc. · PAYGILITY ADVISORS Agility in Payments and FinTech · PAX

PayPal · PUSH PAYMENTS · Qualpay · Syniverse · TableSafe · TINSLEY RETAIL INSIGHTS · UNITED STATES FEDERAL RESERVE SYSTEM · US PAYMENTS FORUM · verizon · vibes

MEDIA PARTNERS

ACT Canada · Banking CIO Outlook · DIGITAL TRANSACTIONS Trends in the Electronic Exchange of Value · eTail · GLC · Money 20/20 · TRANSACT POWERED BY ETA · INCITE GROUP · LendIt Fintech USA · NILSON REPORT · RETAIL executive

Register now at MobilePaymentConference.com

Behind the M&A Boom

Jim Daly

To explain today's mergers and acquisitions in merchant acquiring, mix a hefty dose of technology and a dash of foreign spices with traditional flavors like greater scale. And don't forget a little fear.

For years, greater scale seemed to be the big driver of mergers and acquisitions in the merchant-acquiring industry. Technology, of course, traditionally has been an important factor too. Over the past year, however, access to new technology has become more prominent as processors scramble not only to survive, but also to distinguish themselves in a fast-changing market.

This quest for new technology comes as the cogs that drive the merger machine are humming along quite smoothly in 2018.

"You have a combination of good economy, money, and fear factor—and technology," says payments-industry analyst Lawrence Berlin, a senior vice president at Chicago-based First Analysis Securities Corp.

The nexus of this technology drive is the corps of independent software vendors that develop vast arrays of business-management applications for merchants, many tailored for the point of sale. Acquirers covet relationships with ISVs because such pair-ups can make for more lasting and profitable relationships than traditional price-driven ties.

Acquisition targets with desirable technology and ISV relationships have received buyout offers with some of the highest multiples to pre-tax earnings among recent deals. Examples include First Data Corp.'s acquisitions of Card-Connect Corp. and BluePay Holdings Inc., and the buyout of Cayan LLC by Total System Services Inc. (TSYS).

"The whole focus on ISVs and integrated POS—that continues to be the driving force," says Jared Drieling, senior director of business intelligence at The Strawhecker Group, an Omaha, Neb.-based consulting firm.

Technology and scale, however, don't explain everything occurring today in acquiring-industry M&A. International opportunities are playing an important role in the increasingly globalized payments market, and U.S. companies can be sellers as well as buyers.

In January, suburban Cincinnati-based processor Vantiv Inc. closed on its $11.7 billion acquisition of London-based Worldpay Group plc, with the merged entity now known as Worldpay Inc. ("Let's Make a Deal," December, 2017). And the British processor Paysafe Holdings UK Ltd. in April announced a pending deal to buy iPayment Holdings Inc., a big independent sales organization based in Westlake, Calif.

Still, access to ISVs and their technology comes up as frequently if not more than any single reason driving recent acquiring-industry deals, and that dynamic doesn't seem likely to change any time soon.

"Tech will be a big factor going forward," says Berlin.

'A Lot of Cheap Money'

The tech trend is getting a boost from the still relatively low cost of financing despite recent interest-rate increases from the Federal Reserve.

"Right now, there's a lot of cheap money out there," Berlin says.

A reflection of tech's desirability is the multiples big acquirers are paying for smaller processors and ISOs that have coveted technology platforms and access to ISVs.

The $1.05 billion that Columbus, Ga.-based TSYS paid for Boston-based Cayan, for example, represented a multiple of 21 times Cayan's earnings before interest, taxes, depreciation and amortization (EBITDA), according to an analysis by The Strawhecker Group (chart, page 16).

The Cayan multiple was the highest of the 2017-18 deals examined by the consultancy for which financial data was available. Cayan brought to TSYS 70,000 merchants generating $26 billion in annual gateway and processing volume combined, 100-plus integrated-payments partnerships, and Cayan's so-called Genius platform, a

Financial Comparables in Recent Merchant-Acquiring Acquisitions

(Dollar figures in millions)

Seller	CardConnect	BluePay	Worldpay Group	Merchants' Choice
Buyer	**First Data**	**First Data**	**Vantiv**	**Paysafe**
Year Announced	2017	2017	2017	2017
Value	$750	$760	$11,680	$470
Seller Gross Profit[1]	$65	$175	$1,850	$72
Gross Profit Multiple	11.5	4.3	6.3	6.5
Seller EBITDA[1,2]	$38	$48	$748	$49
EBITDA Multiple	19.7	16.0	15.6	9.6

1. Trailing 12 months.   2. Earnings before interest, taxes, depreciation and amortization.   *Source: The Strawhecker Group*

set of software and hardware tools for merchants. Former Cayan chief executive Henry Helgeson is now president of integrated solutions at TSYS.

"Generally, the tech and ISV concentration is a driver," says Drieling. "These could also be strategic vertical plays."

Such cases could include "a major foothold in a particular, growing vertical" like business-to-business payments, geographic concentration, or tier size such as small-and-medium-size businesses, he says. "In the case of Cayan, they had a little bit of it all, including a tech-focused SMB merchant base."

The Cayan acquisition capped a years-long drive by TSYS to diversify beyond its straight third-party processor origins into a direct player in the acquiring industry. The effort picked up speed in 2011 when it bought the part of a joint acquiring venture with First National Bank of Omaha that it didn't own. It continued through acquisitions of the payment-facilitator processor ProPay Inc. in 2012 and the big ISO TransFirst Holdings in 2016.

For now, TSYS will be focused mostly on digesting Cayan, though it's open to more acquisitions, according to chief executive M. Troy Woods.

"I think we've got a lot of good assets under [our] roof," Woods said at an April 25 conference call with analysts to review first-quarter results, according to a Thomson Reuters StreetEvents transcript. "Now with all that said, we continue to look at opportunities, and we will continue to look at anything that we believe can help us with scale, help us particularly in our verticals, and with our integrated-solution properties."

'Taking Market Share'

Atlanta-based First Data also proved it is willing to open its wallet when it paid EBITDA multiples of 19.7 and 16 for CardConnect and BluePay, respectively.

"We had no presence really in the ISV business a year ago," First Data chief financial officer Himanshu Patel said during the company's April 30 first-quarter earnings call. "We are clearly taking market share in that space rapidly, and the tools that we've acquired through there, through those businesses, are also helping us take share in the broader partner space, which includes agents." He added that "we feel great about those businesses, and we're seeing that in the revenue numbers now."

The acquired brands have consolidated under the CardConnect name, though the BluePay payment gateway remains in place. The technology, operations, and sales teams have been merged, First Data said in May.

Besides outright acquisitions, First Data is willing to invest in companies with desirable technology. It recently participated in a $12 million funding round for Salido Inc., a restaurant POS system provider, CNBC.com reported in May.

Square Inc., the upstart of the acquiring industry, is an active player in the restaurant space, having introduced its Square for Restaurants, a POS service, in May. That move came just after the San Francisco-based firm bought Weebly Inc., which provides Web stores for entrepreneurs. That acquisition could boost Square's effort to recruit larger merchants.

Meanwhile, according to its top executives the now-completed merger of Vantiv and Worldpay has created new opportunities for the company to export legacy Vantiv's extensive ISV systems and expertise first to the United Kingdom, legacy Worldpay's home field, and ultimately to the rest of Europe.

A pioneer in ISV payments, Atlanta-based merchant acquirer Global Payments Inc. has not announced any major deals this year. It is, however, exploiting some of the opportunities it gained last September when it bought from Vista Equity Partners two major units of the Active Network, a provider of management software for event sponsors, for $1.2 billion.

Along with Active, Global gained access to Vista's approximately 45 portfolio companies as the private-equity firm's preferred payments partner, opening a door for it to offer integrated payments to business-management software developers.

(not identified)	(not identified)	(not identified)	(not identified)	Total Merchant Services	Cayan
(not identified)	(not identified)	(not identified)	(not identified)	North American Bancard	TSYS
2017	2017	2017	2017	2017	2018
$250	n.a.	$450	$50	n.a.	$1,050
$78	$42	$69	$20	n.a.	$150
3.3	0.0	6.3	2.3	n.a.	7.0
n.a.	n.a.	$38	$6.7	n.a.	$50
n.a.	n.a.	11.3	6.7	n.a.	21.0

Last month, Global struck a deal with RA Outdoors LLC, which does business as Aspira, under which it will provide payment services. Dallas-based Aspira provides software for reservations and other campground-management tasks, and for hunting, fishing, and recreational-vehicle licensing.

"This is the third Vista portfolio company to select Global Payments as its partner in as many quarters," Global chief executive Jeffrey S. Sloan said on a May 3 conference call with analysts to review first-quarter financial results. "As we discussed in our February [earnings] call, we continue to invest in leading-edge technologies to accelerate growth of product distribution and to provide seamless connectivity to our customers and partners in an increasingly complex world."

International Expansion

The apparent biggest acquiring-industry deal announced so far this year is Paysafe's pending acquisition of iPayment, which could close this month. This deal puts more focus on market share and international expansion than on tech.

Though the parties did not disclose financial terms, iPayment serves more than 137,000 merchants and processes in excess of $28 billion in volume annually—likely indicators that the company won't come cheap.

Last year, Paysafe laid out $470 million in cash to buy Shenandoah, Texas-based Merchants' Choice Payment Solutions, which processes for 60,000 mostly small and mid-sized merchants generating $14 billion in volume. With the addition of iPayment, Paysafe will rank as one of the five largest U.S. non-bank payment processors, the company said in April.

"Paysafe has been on an acquisition path for the past couple of years and iPayment was a strong strategic fit," a Paysafe spokesperson says by email.

Paysafe itself was acquired last December when private-equity firms Blackstone Group LP and CVC Capital Partners took the firm private in a deal valued at $3.89 billion.

But don't forget a dash of fear, too, as analyst Berlin mentions. Specifically, the fear by acquirers of not having the technological resources needed to compete. That fear can drive deals.

"Where people are fearful is because of the technological shifts," he says. **DT**

—With additional reporting by Kevin Woodward and John Stewart

The Shared Checkout's Slow Check-in

John Stewart

Sky-high abandonment rates, PayPal dominance, and a new online standard are pushing the major card networks toward a common buy button. But don't look for that to emerge any time soon.

When the major card networks in April started talking about what they called a common buy button for e-commerce, observers of the payments industry could be forgiven for wondering what was up.

After all, Visa Inc. and Mastercard Inc. had made heavy investments in time and money trying to establish Visa Checkout and Masterpass, their respective digital wallets. Mastercard, indeed, reintroduced Masterpass only two years ago as part of a brand refresh. And Visa in 2014 did much the same for Visa Checkout, which had been laboring under the name V.me.

Yet none of the network checkouts has been measuring up to PayPal Holdings Inc., which claims a much larger share of the top 10,000 Web sites globally (chart, page 19). For that matter, even Apple Pay and Alipay are ahead of Visa and Mastercard.

In that context, orchestrating a shared button consolidating online checkouts may seem to make some sense, regardless of the sunk investment in the individual brands. "It doesn't appear they've gotten traction on their own," notes Thad Peterson, a senior analyst at the Boston-based consultancy Aite Group LLC. "It's

smart for them to consolidate to compete with Amazon and PayPal."

'Sketchy Half Statements'

But there's one big cautionary note: Whatever shape this unified checkout takes, the end product will be a long time in coming. With each week that passes, the concept takes on more definition, but despite all the discussion, the idea of an online checkout shared by multiple payment networks remains too vague—and too futuristic—to suit some expert observers.

"I keep looking for confirmation that they're actually working on this," says Rick Oglesby, principal at payments consultancy AZ Payments Group, Mesa, Ariz. "I keep finding sketchy half statements."

Moreover, questions abound about branding and who will—and will not—be allowed to participate. Will the debit networks, for example, be invited in? If not, will merchants' routing rights be respected?

A few tantalizing hints about Visa's thinking on the matter emerged last month when chief executive Al Kelly confirmed that there are "a lot of meetings going on, on things like branding and what will the actual button look like." But he also said

experts at Visa are "still going through the technical specifications to make sure we understand exactly what we have to do to implement it," according to a transcript of the session.

Kelly made his remarks during a question-and-answer confab with a JPMorgan Chase & Co. analyst at a technology conference sponsored by the bank.

The "technical specifications" mentioned by Kelly refer to the Secure Remote Commerce (SRC) spec recently drawn up by EMVCo, a standards body controlled by six global card networks, including Visa as well as Mastercard, American Express Co., Discover Financial Services, Japan's JCB, and China's UnionPay.

A technical framework for the spec was released Nov. 1, but the spec itself so far is available only to subscribers. The framework spells out a structure that calls for tokenization of online transactions, cooperation with EMVCo's new 3-D Secure protocol to prevent fraud ("Securing the Future of 3-D Secure," July 2016), and a simplified online purchase process for consumers.

One objective, for example, is "[r]educing shopping cart abandonment by decreasing repetitive manual PAN entries." The PAN is the primary account number printed or embossed on each card. Consumers continue to walk away in huge numbers from online sessions at the point of buying,

a point of major frustration for merchants and payment providers alike.

And the problem only promises to get worse. Abandonment rates for mobile phones, which are accounting for more and more online commerce, were 13 percentage points higher than for desktop machines over the busy Black Friday to Cyber Monday weekend last year (chart, page 20). Yet mobile phones are expected to generate $295 billion in worldwide volume by 2020, up from $79 billion in 2016, according to Aite (chart, page 20).

'Very Streamlined, Far Less Friction'

But relief is likely some time off. While TS Anil, global head for payment processing products and solutions at Visa, said publicly last month that the card company will begin moving its digital wallet, Visa Checkout, to the SRC standard late this year, some observers
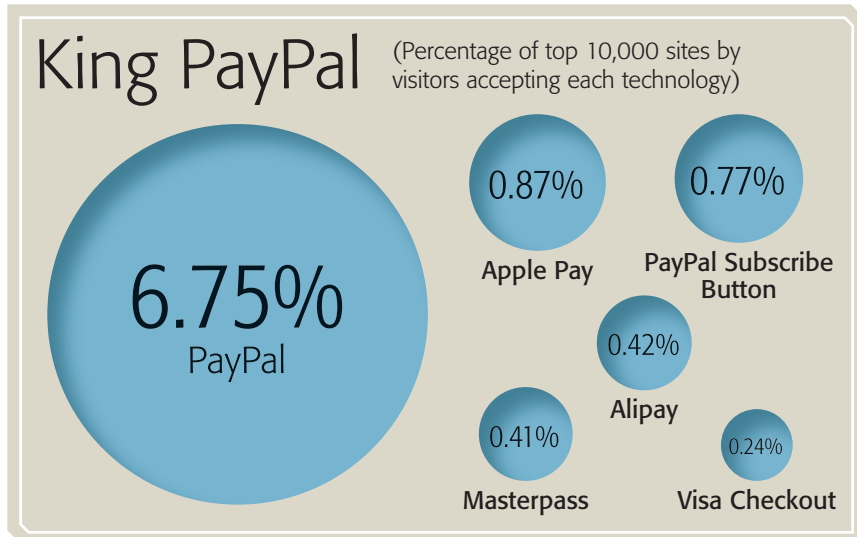
estimate full implementation of a common checkout will take much longer. Aite's Peterson, figures the effort will take three to five years. "It's not going to be fast," he says.

Why so long? The details to be worked out are many and complex,

and that working-out process depends on agreement among EMVCo members that entertain conflicting interests and competitive agendas.

For his part, Kelly ventured some general speculation at the JPMorgan conference on how the common

King PayPal

(Percentage of top 10,000 sites by visitors accepting each technology)

6.75% PayPal

0.87% Apple Pay

0.77% PayPal Subscribe Button

0.42% Alipay

0.41% Masterpass

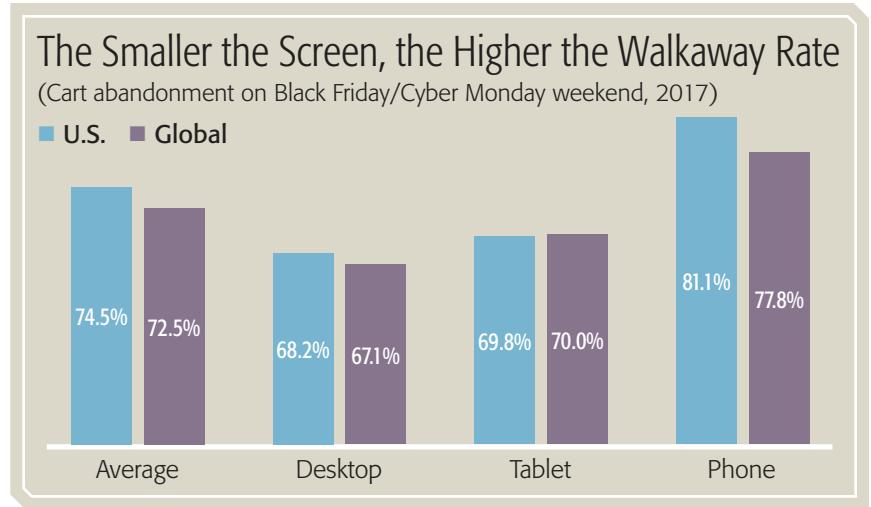**0.24%** Visa Checkout

Source: Similartech.com

button might work with respect to branding. "It'll be ... like in the physical [point-of-sale] world where there's a number of networks represented on the same decal, it'd probably be something similar to that," he noted.

As for the common button's interaction with consumers, Kelly had this to say: "They don't have to look at all the various options and buttons they see, some kind of buy button yet to be defined and branded. It'll open up a wallet. They'll have probably a card preselected. They can override that, select their product and confirm their purchase. Very streamlined, far less friction ..."

The question is, says Oglesby, who will control that wallet that opens up? And if it opens access to any wallet enrolled by the consumer, he asks, who controls that enrollment?

Other parties, too, are waiting for more definition of the networks' unified-checkout approach. Merchants, for example, fear the big card networks may shut them out of the development work and possibly disregard their routing rights when it comes to debit checkouts.

The very fact that the SRC specification is available only to subscribers on the EMVCo Web site is disturb-

The Smaller the Screen, the Higher the Walkaway Rate
(Cart abandonment on Black Friday/Cyber Monday weekend, 2017)

■ U.S.　■ Global

	Average	Desktop	Tablet	Phone
U.S.	74.5%	68.2%	69.8%	81.1%
Global	72.5%	67.1%	70.0%	77.8%

Source: Barilliance

ing in the face of Visa's statement that it wants to act before the end of the year, says Laura Townsend, senior vice president of operations for the Merchant Advisory Group, a Minneapolis-based trade group for major retail chains and airlines.

"It's a speed-to-market challenge for merchants that have their own pay buttons," Townsend says. And yet, she says, "We don't have access to the spec." Rugged as the road to a common buy button may be, the big networks have one key advantage, she argues. "Those who own EMVCo have the advantage of being best prepared to roll SRC out quickly," she

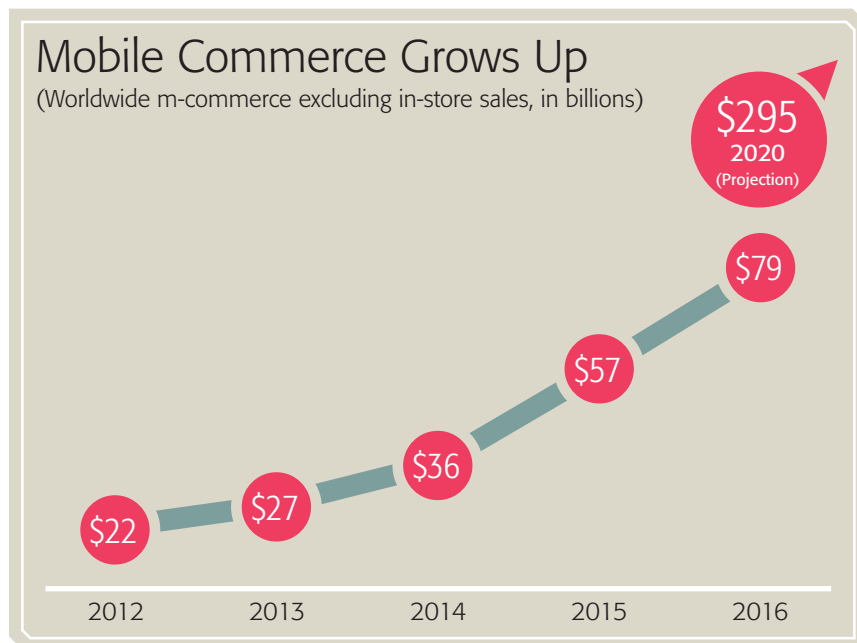says. "Anyone who's not a major brand is at a disadvantage."

At least some debit networks, too, view the move to SRC and a common checkout with skepticism, having recently battled the big card networks over chip-based debit card transaction routing. "We are seeking to understand what EMVCo is going to allow, who they are going to allow" under a unified checkout scheme, says a spokesman for the Johnston, Iowa-based Shazam network in a prepared statement for *Digital Transactions*.

'The Experience Stinks'

Regardless of how long it takes to create a streamlined, online checkout that serves for all or even some interested payments parties, the networks concede they must act soon, before cart-abandonment rates become even more dismal and PayPal and Amazon.com Inc. open up an even wider market-share gap over Visa Checkout and Masterpass.

The proliferation of acceptance marks online doesn't help, especially on small mobile screens. "What we have today is the moral equivalent of having to ask a face-to-face merchant to have a different terminal for each network," Kelly said at the JPMorgan conference. "Imagine the confusion at the point of sale if you had seven or eight terminals."

Summing it up for merchants and consumers, he added, "the experience stinks." **DT**

Mobile Commerce Grows Up
(Worldwide m-commerce excluding in-store sales, in billions)

$295
2020
(Projection)

$79

$57

$36

$27

$22

2012	2013	2014	2015	2016

Source: Aite Group

THE BANKS STRIKE BACK

Keeping track of the players in peer-to-peer payments is like following an ensemble cast—a playbill is needed to identify all the companies jumping in.

From fintechs to financial institutions, P2P is hot. Among the fintech innovators looking to carve out a piece of the P2P pie are such giants as Google LLC, Apple Inc., Square Inc., and Facebook Inc. Even Amazon.com Inc. is rumored to be looking to dip its toe into the P2P waters. Many of these players have taken the plunge by integrating P2P payments into their respective mobile wallets.

And don't forget Venmo, the perennial favorite among Millennials that PayPal Holdings Inc. acquired in 2013. Among fintechs in the P2P space, Venmo has captured the most volume, processing $35 billion in payments in 2017.

Venmo's volume pales in comparison, however, to that of Zelle, a collaborative effort by some of the nation's largest banks to create the pre-eminent P2P service in the United States.

Zelle racked up $75 billion in transaction volume in 2017, and shows no signs of slowing down: Volume totaled more than $25 billion in the first quarter, a 15% increase from the fourth quarter of 2017. At the same time, the number of transactions also shot up, totaling 85 million, up 14% from the fourth quarter.

'PLENTY OF VOLUME'

So, after years of languishing in the shadow of the tech players, have the banks finally found the key to cracking the P2P code? Not so fast. Industry experts are quick to point out that P2P has only begun to scratch

the surface of cash and check volume, which is at least a $1.2 trillion market, according to Boston-based Aite Group.

With so much volume at stake, many payment experts believe that fintech providers will not only survive, but thrive. "Banks have the majority of the volume right now, but there's plenty of volume for everyone," says Talie Baker, a senior analyst for Aite. "There are a lot of other players than banks that are growing rapidly."

Indeed, just in December 2017 alone, Square generated $90 million in transaction volume on its Cash Card, which enables consumers to send, receive, and spend cash from the Square Cash app. At that rate, Square projects the Cash Card will generate $1 billion in annual transaction volume. There were more than 7 million monthly active customers in December 2017, the company says in its annual report.

And Venmo is still red-hot. Its annual volume grew 97% in 2017 and topped more than $12 billion during the first quarter of 2018, up 80% over the same period in 2017. It was the second time Venmo's quarterly volume exceeded $10 billion, the first occurring during the fourth quarter of 2017, when volume hit $10.4 billion.

Certainly, Zelle's quick success has tightened banks' grip on a business many observers say they should have owned all along. But, given the fast growth players like Venmo, Zelle, and Square are experiencing, controlling this market is only part of the challenge. Equally pressing are the questions of how P2P providers can differentiate themselves, sustain their upward trajectories, and find profits in a business where consumers expect the service to be free.

For non-bank P2P players, the key to ongoing success in the near-term, payments expert say, will be to add features that enhance the cool factor of their apps, such as expanding usage to the point of sale and adding more social-media experiences.

Zelle, meanwhile, will continue to rely on the strengths the banking system can provide

consumers: interoperability between member banks, real-time transfer of funds directly into bank accounts, and consumer trust in the banking system's ability to digitally move money safely.

"The goal for Zelle is to make the customer experience around P2P frictionless and ubiquitous so it becomes natural to make real-time payments through Zelle," says Ian Macallister, vice president of sales and customer success at Scottsdale, Ariz.-based Early Warning Services LLC, which operates Zelle. "We are looking to build consumer confidence in the Zelle network."

'MOBILE-BUYING EXPERIENCES'

The fintech payment apps haven't slacked off in the face of Zelle's landing with such force in their midst. As part of its push to evolve the customer experience, Venmo has been devising new ways for users to split and share payments.

In April, Venmo teamed up with online and mobile takeout food-ordering marketplace Grubhub to allow diners to pay their portion of the bill directly to Grubhub when placing an order through its Grubhub, Seamless, or Eat24 apps.

Before, Venmo users split the tab by having one person pay it and then collect from his friends through the app.

Once a consumer makes a purchase using a Grubhub app, the purchase automatically appears in the consumer's Venmo app with the option to split the payment among multiple parties, provided everyone in the group has Venmo.

"This makes it easier for friends to pay for and split group food orders using Venmo," says a PayPal spokesperson. "Food is a top

ZELLE VS. VENMO

(Quarterly volume, in billions)

	Q1 2018	Q4 2017	Q3 2017	Q2 2017	Q1 2017
Zelle	$25	$22	$17.5	$16+[1]	$16+[1]
Venmo	$12	$10.4	$9	$8	$6.8

1. Estimate. Total volume for Q1 & Q2 2017 was $33.6 billion. During that period Zelle was known as clearXchange. Rebranding took place Q2 2017.   Source: Company reports, Digital Transactions

use case for our customers, with pizza the most-used emoji, so we're bringing the social-payment experience our customers love to the mobile-buying experiences we know they already enjoy."

Venmo allows users to attach an emoji as part of its messaging capabilities. As for Grubhub, digital payments are not new as the company already accepts PayPal.

Since more than 60% of Grubhub's orders are placed using a mobile device, Grubhub says it is looking for ways to make it easier for its users to find and order food they want, when and where they want it. "Adding the 'split-the-bill' feature provides an additional level of convenience our diners have come to expect from us," Sam Hall, Grubhub's chief product officer, said in a prepared statement.

'A UBIQUITOUS DIGITAL WALLET'

In many ways, the Grubhub deal builds on Venmo's strategy of evolving itself from being just a P2P app to a payments platform. Venmo took a major step in that direction last fall when it announced Venmo users could make purchases at more than 2 million retailers that accept PayPal for purchases in the United States. PayPal's merchant base includes Walmart, Target, Lululemon, Forever 21, and Foot Locker.

"Offering a way to pay at millions of retailers is a major step in the evolution of Venmo," Bill Ready, chief operating officer of PayPal, said at the time of the announcement. "Our vision for Venmo is to not only be the go-to app for payments between friends, but also a ubiquitous digital wallet that helps consumers spend wherever and however they want to pay, regardless of device."

While the move makes it possible for PayPal to monetize Venmo by charging merchants acceptance fees on purchases, it's significance reaches much further, because consumers have the option to share their activity on Venmo's social-media feed, along with any messages that accompany the transaction.

That's something most Venmo users opt to do. Chip in on wedding-shower gifts using Venmo, and it's there for others to see. Go out for a drink after work with friends, and Venmo provides the details.

That level of information sharing can also work as a viral form of marketing for merchants accepting Venmo payments, says Richard Crone, principal at Crone Consulting LLC, a San Carlos, Calif.-based financial-services consultancy.

"Sharing with friends the name of the merchant where you just made a purchase is an endorsement for that merchant," Crone says. "Merchants already ask consumers to like them on Facebook, and the

> 'THE GOAL FOR ZELLE IS TO MAKE THE CUSTOMER EXPERIENCE AROUND P2P FRICTIONLESS AND UBIQUITOUS.'

byproduct of accepting Venmo is word-of-mouth marketing. Merchants will pay for that exposure.”
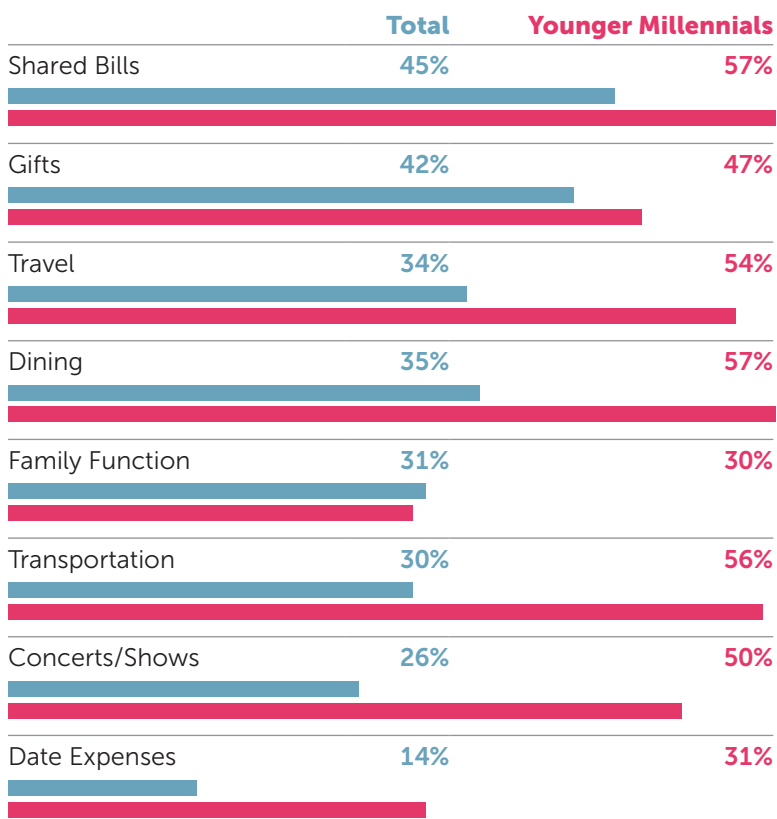
Social-media marketing is very popular among Millennials, who have few qualms about sharing details of their lives in the online world, and who have been known to keep tabs on what their friends are up to through Venmo. Besides being heavy users of P2P apps—four out of five young adults in the U.S. use P2P, according to Maynard, Mass.-based Mercator Advisory Group—this demographic also pays attention to the wisdom dispensed by so-called influencers who use social media to make their opinions about merchants known.

“Seeing what their friends are up to through social media is important to those under the age of 30,” says Rachel Huber, an analyst with Pleasanton, Calif.-based Javelin Strategy & Research’s payments practice. “Why wouldn’t a merchant want a Pay with Venmo button to get free promotion through Venmo’s social ledger?”

But not all payments experts are sold on the notion that social-media marketing will provide a big lift to merchant sales. While Venmo users are comfortable sharing information about their purchases, the success of Zelle, which includes the option to attach a note to each payment but offers no social-media experience, suggests that social media are not necessarily a must-have when it comes to P2P payments, argues Norm Marraccini, vice president of product management, digital payments, for Fidelity National Information Services Inc. (FIS), which resells Zelle to financial institutions.

‘SEEING WHAT THEIR FRIENDS ARE UP TO THROUGH SOCIAL MEDIA IS IMPORTANT TO THOSE UNDER 30.’

Zelle, like Venmo and Square Cash, is targeting consumers in their mid-20s to early 30s, the group that is the heaviest users of P2P payments.

WOW FACTOR

Business-to-consumer payments is another feature P2P providers have been developing. In March, Square began enabling direct deposits of paychecks to Square Cash users’ accounts.

To initiate the service, Square Cash users need only provide their employer their account and routing numbers. Users are notified as soon as the funds hit the account. Square announced the service over Twitter with the headline Payday! accompanied by a bag-of-cash emoji.

“Square Cash has been at the forefront of the digital P2P payments movement since inception, and per the media, has been a solid competitor to companies such as PayPal and Venmo,” Aite’s Baker said in a report titled “Digital Person-to-Person Payments in the U.S.: The Competitive Landscape.” She continues, “Square has become a brand recognized for innovation that challenges the status quo.”

Square Cash users are charged a 1% fee to withdraw money the same day it’s received. Users preferring to avoid the fee can wait until the next business day to get their money. Users can also use the app to make purchases through merchants, which generates transaction revenues.

Square isn’t the only P2P provider pushing to transition to a full-fledged payments platform. Last December, Apple introduced the Apple Pay Cash card. Consumers making P2P payments

P2P IN ACTION

(What P2P users are paying for with P2P transactions)

	Total	Younger Millennials
Shared Bills	45%	57%
Gifts	42%	47%
Travel	34%	54%
Dining	35%	57%
Family Function	31%	30%
Transportation	30%	56%
Concerts/Shows	26%	50%
Date Expenses	14%	31%

Source: Bank of America Trends in Consumer Mobility report

through Apple's Messages messaging platform can send or receive funds using the card, which is issued by Pasadena, Calif.-based Green Dot Corp., an issuer of prepaid cards. Transactions made with the card run over Discover Financial Services' network. Neither Apple nor Discover would comment for this story.

Another wow factor making its way into P2P payments is voice activation. In March, Google announced in a blog post it was adding Google Pay to its Google Assistant. Google Pay users can send or request money from their contact list using Google Assistant on Android and iOS phones in the U.S. P2P transactions are free. Down the road, Google Pay users will be able to send money on voice-activated speakers such as Google Home.

"We're embedding P2P into apps that people use every day and many times in the context of exchanging value, such as Android Messages and Gmail," a Google spokesperson says. "Our focus is on providing users the best and most delightful experiences that allow them to pay others however they like."

Google Pay recently passed the 100-million milestone for downloads, the company says.

FIS is also looking at ways to incorporate voice activation into its People Pay P2P app, Marraccini says. Those features most likely won't be available until 2019 at the earliest.

'A COMMON BRAND'

But if the non-bank players aren't standing still, neither are the nation's biggest banks. Unlike many of its competitors, Zelle is not scrambling to add more bells and whistles to its core offering. Instead, banks are making Zelle a core feature of their mobile-banking applications.

"P2P payments are table stakes in mobile banking now," says Mark Monaco, head of enterprise payment for Charlotte, N.C.-based Bank of America, one of Zelle's founders. "Zelle is a tool to make payments more mobile and digital, which fits with how people are increasingly living their lives and interacting with others."

As it stands, Zelle is primed to push into business-to-consumer payments, such as disbursements for insurance payouts. Making such payments digitally can significantly reduce the cost of writing, sending, and processing a check, which can run between $4 and $5, says Macallister. Reducing that cost is

FREQUENCY FOCUS

(Annual P2P payments, among users making one or more P2P payment in 2017)

Source: Aite Group

52%
1 to 3 payments

2%
10 or more payments

15%
7 to 9 payments

31%
4 to 6 payments
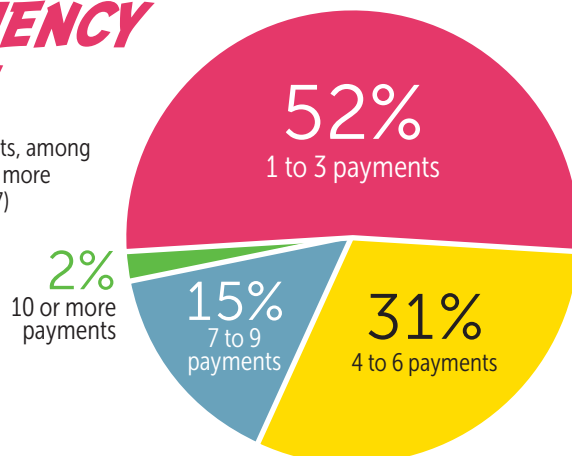
a service businesses will pay for, provided the cost is substantially less than what they pay now, payments experts say.

While some Zelle members are reportedly moving into, or planning to move into, the B2C arena, the immediate focus for Zelle remains to drive adoption and increase volume. That's why Zelle and its members have embarked on a marketing strategy of creating a ubiquitous network brand that banks can promote as the engine behind their P2P apps.

"Our member banks have their own brand and we don't want to undercut those brands," says Macallister. "Our aim is to create a common brand that banks can leverage as they choose when marketing their mobile-banking services."

Bank of America, for example, promotes Zelle as a way to send money quickly and securely within its mobile-banking app and through its Web site.

BofA, which has about 3.5 million Zelle users who have made at least one transaction in the past 30 days, offers users the option of splitting a bill between multiple contacts, such as a group dinner check, and the ability to add a personal note along with the payment transfer or request.

'IT'S THE FUTURE'

Despite all the maneuvering by P2P providers to dazzle customers and get them comfortable making a P2P payment, the big question for all P2P providers is whether they can make the service profitable. By making P2P free to consumers, payments experts agree that P2P providers let the genie out the bottle and can't put it back.

So how can P2P providers monetize their services? Besides expanding P2P to the point of sale, which nets merchant fees, some providers such as Zelle and Square are betting P2P is a gateway to services that can be monetized, such as loans and other financial services for which they can charge.

"Zelle doesn't have to be monetized, because it successfully deepens customer relationships and opens the door to offer users other revenue-generating products," says BofA's Monaco.

However P2P providers look to make money, they can all be counted on to jazz up the consumer experience, because that what's going to onboard more consumers and get them to shift their spending away from cash and check.

"P2P payments provide value, speed, convenience, and secure payments," says Monaco. "It's how people increasingly want to engage when it comes to payments. It's the future." DT

The Unwelcome Guest

Kevin Woodward

Merchants using hospitality point-of-sale systems face a relentless onslaught by wannabe hackers coveting their payment data. What can put an end to it?

Hospitality merchants, such as restaurants, bars, and entertainment venues, know that an effective point-of-sale system can help them operate their businesses better. They can glean valuable information from their transactions about which products are selling best, the average ticket value, and other data.

The bad thing, however, is that criminals know this. They have only one mission: Steal the payment data and anything else that might help them plunder merchants and consumers.

Indeed, the point of sale is the number-one avenue hackers use to get to payment data among hospitality merchants. Point-of-sale intrusions represent 96% of all data breaches in the accommodation and food-services segment, according to Verizon Communications Inc.'s latest breach study.

Data like this is not unique to a single breach investigator. Trustwave Holdings Inc. said 11.9% of the breaches it investigated in 2017 were in the hospitality segment. Among the breaches in the hospitality segment, 78% sought card track data, the highest percentage among nine segments included in the 2018 Trustwave Global Security Report.

Few envision a quick abatement of the onslaught. "The hospitality market is a big focus area for the cybercriminals, especially from the data we're seeing," says Michael Aminzade, vice president of the global compliance and risk service at Chicago-based Trustwave. "Criminals deem the hospitality vertical a weak area from the mature cybersecurity space."

'Hacker Folklore'

Criminals see hospitality POS systems as easier targets than some other sectors because there often is a lack of investment in upgrading systems. Legacy operating systems continue to be used, and many merchants extend the upgrade cycle as long as possible, Aminzade says.

Part of the reason for the delayed action or inattention by merchants is that they often are more focused on upgrading their POS systems to improve the customer experience, he says. The costs of upgrading, and adding such measures as integrated EMV acceptance, increases the complexity for merchants, Aminzade says.

Overall, security is not top-of-mind. Says Erick Kobres, chief technology officer at Revel Systems Inc., a San Francisco-based tablet POS

system provider: "Until you get to the enterprise customers, frankly, [merchant awareness] is pretty poor. Merchants are focused on running their businesses. Security is highly technical, not very exciting, and tends to [rank] low on priority lists until they've been breached."

Like many POS system providers, Revel Systems provides education to merchants. It tries to hammer on the importance of security, Kobres says, but sometimes the message doesn't come through as hoped.

The lack of security best practices among hospitality merchants exists "across the board," says Marc Punzirudu, director of security consulting services at ControlScan Inc., an Alpharetta, Ga.-based data-security provider. "There are some organizations over the last couple of years that have broken the mold, but generally speaking, it's still not where it should be," he says.

In Punzirudu's estimation, one key best practice is to avoid ranking the information technology director below the chief financial officer. Following that practice "really shows the executives' prioritization of security in the [profit and loss] statement," he says.

Merchants continue to have antiquated remote-access protocols, fail to patch software, and run multiple functions from the point-of-sale server. "One email is all it takes to put malware on a POS server, which

most likely has clear-text payment card data in memory—or at least has access to a POS terminal."

Criminals favor hospitality POS systems for another reason beside the appeal of the payment and customer data: the ease of getting the data out of the systems. "Exfiltration of the data is easy for a criminal, as typically the firewall rules are not specifically preventing communications to sources which are not required for operations," Punzirudu says.

Locking down what goes in and comes out of a device handling payments is one reason why Revel Systems uses Apple Inc. iPads for its POS service. "Our products are turnkey," Kobres says. "We take a number of measures to protect ourselves and our cloud infrastructure." Among them, of course, are PCI compliance and EMV acceptance, to help with fraud mitigation, and point-to-point encryption.

"Hospitality is such a big target because historically it's been a lucrative environment, especially for organized crime, to target," Kobres says. "Not that many years ago, it wasn't uncommon for criminals to break in and get access to a PC at a manager's workstation and have access to tens of thousands of card numbers."

The advent of the PCI Security Standards Council's data-security standard helped reduce the amount of clear-text payment data stored in POS systems, but that takes time. "Breaking and entering to steal a PC wasn't uncommon five to six years ago," Kobres says. It often involved low risk with a high rate of payback, he says. "That's the story that hacker folklore is made of."

Attitude Adjustment

So what can be done? EMV and the advent of point-to-point encryption have had a major impact. "Getting that deployed has probably been the best thing to happen from a card-fraud perspective," Kobres says.

(Photo: Revel Systems)

'The attacks have gotten easier to launch and criminals have better access to hacking tools.'

—ERICK KOBRES,
CHIEF TECHNOLOGY OFFICER,
REVEL SYSTEMS INC.

Another tactic, which many have advocated and practiced for years, is educating merchants about the perils of poor security practices. But with scores of other business needs demanding attention, merchants, especially smaller ones, lack the time and financial or staffing resources to properly manage POS-system security.

But for those who take the time, there are some elements to look for when evaluating POS system vendors. "Protect the data that is important to you," says ControlScan's Punzirudu. "Payment card data is almost always a concern, so encrypt it using a [point-to-point encrypted] validated card-acceptance method where possible."

Use tokenization services, which mask the actual card number with a string of unrelated digits. This is especially important when card data needs to be stored, which Punzirudu recommends not doing unless it's necessary,

such as for adding a gratuity or other batch-processing actions.

"Your POS server is only your POS and payment-application server," he says. "It is not there for managers and others to check email, read Word or Excel documents, and other administrative tasks."

The rationale for that is simple. "Being that almost every security-research firm and individual will agree that malware is an issue, why would you permit two of the most likely candidates (email and untrusted files) to be opened on those systems in the first place?" Punzirudu asks.

Kobres urges merchants to use a Wi-Fi network solely for its POS system. "You never want to have the POS terminal on the same network as the customer Wi-Fi," he says. "That's an easy one for smaller merchants to overlook."

Security comes down to using multiple layers to protect the data. It's

important to make sure computer ports are not open for surreptitious services to exploit. "By default, an iOS device has no services running on it, unlike Windows or a Linux workstation," says Kobres. A lot of software that operates on Windows, the popular computer operating system from Microsoft Corp., rely on services to function, he says.

Protecting hospitality POS systems also depends on staffing, says Trustwave's Aminzade. Not having a trained person in charge of safeguarding the integrity of the system or failing to use a trusted vendor does the merchant no favors.

Getting past that might require a change in mindset, Aminzade says. "It's just that they need to adjust their attitude and embrace some of the concepts like security by design, privacy by design, and investment strategies that support these over the next three to five years," he says. "They're very quick to support digital innovation, like Wi-Fi in hotel rooms, but they need to put cybersecurity on an equal priority."

Relentless Attacks

All of these best practices will only grow in importance as criminals seek out ways to validate the scads of
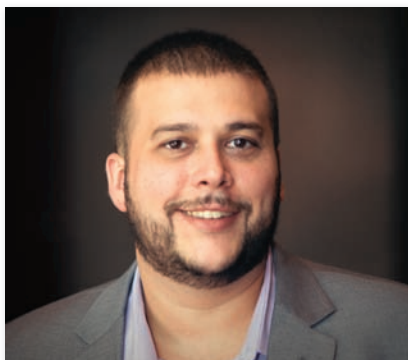
stolen personally identifiable information and payment data.

Ransomware is especially malicious because, when activated, it places the infected devices in lockdown until a fee is paid. Many times, the ransomware is part of an email or file an employee unknowingly opens.

In 2017, according to Trustwave, two high-profile ransomware worms

'I still see a general lack of best practices in hospitality across the board.'

—MARC PUNZIRUDU, DIRECTOR OF SECURITY CONSULTING SERVICES, CONTROLSCAN INC.

were WannaCry, which exploited unpatched computers and those using older Windows operating systems, and NotPetya, which spreads across a network using shared folders and legitimate Windows components and tools.

"I still see a general lack of best practices in hospitality across the board," says Punzirudu. "Adoption of general data-security best practices is still miles off within many restaurants and restaurant chains. There has been a steady increase in [point-to-point encryption] and [end-to-end encryption], which is great for protecting payment card data, but there is still a mountain to climb."

Not only do payments providers and security vendors continue to get more secure POS systems deployed, they, like merchants, have to contend with the relentless and evolving criminal attacks.

"I don't know if we'll see a drop-off in attacks," says Kobres. "The attacks have gotten easier to launch and criminals have better access to hacking tools. The good news is that information is not there to be disclosed. If someone breached our system, there's no card data there." **DT**

Having a trained security person in charge is crucial.

—MICHAEL AMINZADE, VICE PRESIDENT OF THE GLOBAL COMPLIANCE AND RISK SERVICE, TRUSTWAVE

It's Zero Hour for GDPR

Now that the massive regulation is in force, there's no time to waste on getting compliant, says Greg Sparrow.

The General Data Protection Regulation (GDPR) has raised a number of questions for U.S. businesses since its inception on April 27, 2016. After the bill was passed, it was allotted a two-year grace period for businesses to strategize and implement their compliance approach. Even so, one month before the May 25 compliance deadline, it was reported that an estimated 61% of U.S. businesses were not ready for the regulation, and only 67% of European-based businesses had begun moving into the implementation phase of their GDPR compliance program.

The potential fines have many U.S. executives concerned about compliance. But businesses are struggling with fully understanding the regulation and thus have failed to launch a comprehensive plan.

Turning our focus to the retail industry, several chains have displayed international influence with the presence of not only brick-and-mortar stores in several nations, but through international marketing efforts. A well-known example is Whole Foods, an American supermarket chain that previously held over 477 stores in North America and the United Kingdom. After Amazon's acquisition of the natural-foods company in June 2017, the e-commerce giant became America's fifth-largest grocery retailer.

Outside of the benefit of concrete locations near its customers, the marketing data obtained through the acquisition provided Amazon valuable behavioral statistics on grocery-buying habits, patterns, and product preferences. It is estimated that over 80 million individuals are Amazon Prime members and, with this new data, Amazon can build accurate predictive analytic models that can suggest to prime members what they will want, how much they will want, and when they will want it.

The GDPR places Amazon's acquired Whole Foods business unit under scope for not only its presence in the United Kingdom, but also due to its monitoring of European Union (EU) data subjects and attempts to offer them goods and/or services.

Amazon's practices most likely include the use of automated individual decision-making against EU data subjects, requiring explicit consent under the GDPR. Processing is broadly defined in the regulation to include most actions that can be performed with data and can specifically refer to collection and storage, which Amazon in this case would be doing. The massive retailer must therefore have processes in place to honor nine distinct rights awarded to EU data subjects, and be able to operate under the guiding privacy principles defined within the GDPR.

'Expansive Requirements'

The regulation further dictates appropriate security efforts for the protection of personal data, establishes breach-reporting requirements, and increases the risk associated with vendors

Greg Sparrow is senior vice president and general manager at CompliancePoint, Duluth, Ga.

processing this data. These expansive requirements make the process of marketing and vendor outsourcing much more complex for anyone with a direct consumer relationship with EU data subjects.

More specifically, retailers that use customer information from operations such as payment histories must also be careful with the use of this information. This can not only affect these retailers directly, but also any vendor partners that share in the use of this type of customer data for target-marketing intelligence purposes.

Many smaller agencies may not be considering the new regulations as seriously as they should be, but it's clear they could pay a high price for that neglect. Past enforcement actions point to enforcement risk even with smaller agencies. The GDPR states that non-compliant companies posing a risk to EU citizens and their privacy can be fined up to $20 million, or 4% of their global turnover for the previous fiscal year, whichever is greater.

Big companies like Amazon, with net revenue around $178 billion in 2017, could potentially face a fine of $7.1 billion. It is important to note that this fine would be per violation. It can certainly be assumed that larger repercussions would be likely in this hypothetical case, since case law suggests similar types of violations do not stand alone, and typically occur with others.

Risk Mitigation

If they haven't already, there are several steps that companies must immediately embark on to mitigate their exposure to risk. A solid start is to understand GDPR's applicability to various parts of the business, which includes understanding each unit's risk profile to establish priorities for the initiative. Once risk and priorities have been identified, it is critical for organizations to identify and establish their lawful basis for processing customer data.

Every industry has its own unique risk and operational challenges, and every business within has its own maturity relative to industry peers. The unbiased eyes of outside counsel may help to quickly identify both industry and organizational risks that are often otherwise overlooked.

Things could soon get more complex. Some have suggested the GDPR will set a global precedent for data privacy and security regulations. Brazil and China have both shown interest in forming similar requirements to protect the privacy of its citizens' personal information from businesses that store data and transfer it across borders.

To adequately prepare for the GDPR and similar regulations likely to be introduced in the future, businesses must begin educating themselves on these regulations and work out how they will choose to conquer the requirements. Applicable processes and procedures can obviously help minimize exposure to fines. But an added benefit is that they also provide an opportunity within the market to reassure customers and, in return, earn their trust. **DT**

AN OPPORTUNITY AS BIG AS YOUR DREAMS!

At Electronic Merchant Systems our agent partnering approach stems from the understanding that our success is based upon your success. We are committed to building a lasting relationship with you and strive to provide you with the personal service that you deserve from an Agent partnership with EMS.

Google Reviews
600+
Customer Reviews
★★★★★
4.7 Star Rating

Agile Contracts

We understand that we have to earn your business everyday. Our non-exclusive Agreements will be structured to help you dramatically build your business.

Lifetime Residuals

You start earning residuals day one and continue to earn them for as long as the merchant continues to process with EMS. No quotas or any other Gotchas.

Success Assurance

EMS agents are assigned a Success Manager that is your direct connection to EMS. Your Success Manager has your success as mission first and will provide invaluable internal assistance allowing you to do what you do best ... sell.

Portfolio Management

MyPortfolio is a powerful, flexible and incredibly simple to use portfolio management system. Because we understand that transparency is the key to success, we're able to provide you the most complete and current data for your specific business needs.

electronic merchant systems® | AGENT

www.emsagent.com

Call Today!
866.887.8907