DIGITAL TRANSACTIONS®

Trends in the Electronic Exchange of Value

BATTLING THE BOTS

A swarm of malicious bits of code threatens to plunder online assets. What's to be done?

B BANK

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

Best-in-Class POS Solutions For Every Industry

HARBORTOUCH CHECKOUT

A powerful and easy-to-use retail offering that hits the sweet spot for the vast majority of retail businesses. It delivers all the features retailers need in an intuitive and user-friendly software package.

HARBORTOUCH BAR & RESTAURANT

Harbortouch has taken its nearly 10 years of experience in POS to custom develop a brand-new bar and restaurant software, featuring EMV with tip adjust, online ordering, online reservations and tableside ordering.
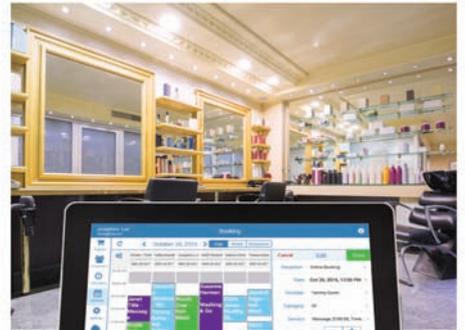
HARBORTOUCH SALON & SPA

Harbortouch Salon & Spa delivers an ideal solution to a vastly underserved market, with industry-specific features like appointment setting, walk-in management, multi-station support and email/text reminders.

Harbortouch has pioneered POS within the payments industry, and we now offer best-in-class POS solutions for virtually every industry as part of the original Free POS Program*.

Plus, we offer:
- **$25,000 signing bonus**
- **12X terminal bonuses w/ $400 upfront**
- **Residual splits up to 75%**
- **Lucrative product bonuses**

And Now Offering Cash Discount!

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

Malicious bots are 'something [retailers] haven't dealt with before. For criminals, this is almost as good as going to the bank.'

PAGE 18

CONTENTS

December 2018 ■ Volume 15, Number 12

Cover illustration: Jason Smith

THE GIMLET EYE

Chase Tries Again

One thing that can help put over a new payment technology is backing from a bank or technology company that controls a huge chunk of the consumer universe. But the key word here is "help." Consumers and merchants have to be ready for the technology, as well.

With contactless cards, that readiness may finally be there. Thirteen years ago, when JPMorgan Chase & Co. launched its blink card with hearty fanfare and big ambitions, it wasn't. After lingering in the market like the ghost of a long-forgotten icon, the card finally met its demise in 2014 when Chase mercifully euthanized it.

Circumstances are much better now for a contactless product. The EMV rollout, as messy as it was, finally put terminals capable of near-field communication on the countertops of millions of merchants. The advent of mobile wallets has trained at least some consumers (though not as many as Apple and Google would like) to appreciate the convenience of tap-and-go. And the need for fast throughput in some sectors has only grown more urgent with EMV's leisurely transaction times.

Sensing the opportunity, Chase is back in the contactless card business (see page 6). The market's contours are different now, of course. The cards are so-called dual-interface plastic, meaning they can be inserted into chip-reading terminals or waved at or tapped on them. They are fitted with NFC technology now for fast and secure interactions. And Americans who venture abroad have had a chance to see for themselves how fast contactless has developed in places like the United Kingdom.

Chase's heft in the credit card business—it is the nation's biggest issuer—doesn't guarantee success. It didn't a decade ago. But a swarm of contactless credit and debit cards unleashed across the country can't hurt, and in combination with dual-interface plastic from other issuers might induce more merchants to enable NFC in those EMV terminals they've deployed.

That should help cure the merchant indifference blink encountered. Consumers weren't so sure they wanted or needed the technology either, a problem that in turn might be overcome by growing familiarity with mobile wallets.

Indeed, it's hard to say how much longer physical, plastic cards are going to be with us. A recent report from the global processor Worldpay says wallet usage is growing fast. Its report it focused on online usage of cards and wallets, but it says the population of in-store wallet users in the United States is growing at a 33% annual rate. Of course, while credit and debit cards may dwindle over time, they will be with us for a while yet. It's good to know they will be so much easier to use.

John Stewart, Editor | john@digitaltransactions.net

® PAX

Your Payment Partner of Choice

| E800 | E500 | E600 | A920 |

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.

® PAX

US Headquarters:

8880 Freedom Crossing Trail
Building 400, 3rd Floor, Suite 300
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
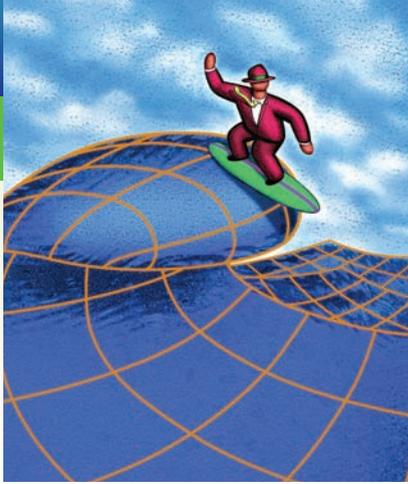
Chase Reconnects With Contactless Cards

Giant card issuer Chase may not be big enough to single-handedly make contactless cards commonplace in the United States, but now that it plans to once again issue tap-and-go credit and debit plastic, the money-center bank could come close.

Chase, a unit of JPMorgan Chase & Co., says it will begin before the year is out issuing contactless EMV cards bearing the Visa Inc. brand, first to its Chase Freedom Unlimited and Chase Slate cardholders as their cards reach renewal or on opening a new account.

Following on will be all other Chase Visa credit cards, including cobranded ones through 2019. In the second half of 2019, Chase contactless debit cards will begin appearing.

Chase said the timing is right because 70% of U.S. merchants have the point-of-sale technology to accept contactless EMV cards. It's the same technology used by mobile wallets like Apple Pay, Samsung Pay, and Google Pay.

Thirteen years ago, Chase, with its blink card, was one of the first to issue a contactless payment card on a broad scale. Those cards relied on magnetic-stripe-equivalent radio frequency technology.

After a failed attempt several years ago, it's contactless redux at Chase.

(Photos: JPMorgan Chase)

Other issuers followed, but contactless payments failed to catch on. The blink brand lingered until its last incarnation was discontinued in 2014. These newest cards use EMV contactless technology to secure the payment data.

Different this time, too, is that one leg of the stool already is in place. Since the 2015 EMV liability shift, point-of-sale terminal makers have shipped their devices not only enabled for contact EMV acceptance, but with near-field communication wireless capability built in.

NFC is the enabling technology for the smart phone-based mobile wallets and for contactless EMV cards.

In September, Visa said 50% of its face-to-face transactions happened at contactless-enabled merchant locations as of June, meaning the merchant's point-of-sale equipment was enabled for, not just capable of, conducting a contactless card payment.

In October, Visa predicted 100 million contactless cards would be issued by U.S. banks and credit unions by the end of 2019. It's an attainable number because of the readiness of the market, suggests Dan Sanford, vice president of product at Visa.

The technology is in place at merchants, and now, with at least one issuer moving ahead and others expected to follow, the payments industry soon can focus on consumers. Part of that consumer message will be the value of using contactless cards, which will retain the contact chip interface, instead of cash, Sanford says.

As other markets, such as Australia and the United Kingdom, added contactless capability to their EMV cards, consumers began using the cards instead of cash, he says. That could happen in the United States.

That's where consumers will have a critical role, not only for using a card instead of cash but to prompt merchants to offer contactless acceptance, says Kevin Morrison, senior analyst at Aite Group LLC, a Boston-based advisory firm.

"It will largely be driven by the spending habits of the average consumer," Morrison says. A consumer who gets accustomed to tap-and-pay at a fast-food restaurant may wonder why a similar experience, which likely will take less time than dipping an EMV card into a reader, can't happen at other merchants, he says.

Card costs also may be a factor. On the low end, the cost may be 50 cents to 60 cents per card, and on the high end between 90 cents and $1.10. Morrison says volume and other elements affect card costs. Even global demand for contactless cards helps lower costs, he says. A contact-only EMV card may cost between 60 cents and 80 cents. Chase would not disclose its costs for the new cards.

Another factor that bodes well is that other issuers are expected to follow Chase's lead. Morrison's research indicates that large and small financial institutions are planning contactless cards, a trend that picked up momentum in the last five months, he says.

"When the big guys move, the little guys don't want to be left [behind]," he says. "There are a number of financial institutions that are going to migrate to this technology. It will take off."

—*Kevin Woodward*

A Startup Player Wants To Be the Common OS for Smart Terminals

Poynt Co., a startup supplier of intelligent payment devices, argues so-called smart terminals should have a common operating system like smart phones do. And in the course of announcing a $100-million funding round last month, the Palo Alto,

Poynt in action: The next OS for smart POS?

(Photo: Poynt)

Calif.-based company also argued it should be the one to provide that OS.

Investors in Poynt's Series C raise include Elavon, a major payments processor and a unit of U.S. Bancorp, and National Bank of Australia. Poynt will use the funds to expand its talent base, invest in its product, and pursue "its vision to become the operating system (OS) on smart payment terminals worldwide," according to a release from the company.

Four-year-old Poynt, whose L-shaped device relies on a collection of apps that can support a variety of merchants' business needs, says it has shipped 150,000 units in the past 16 months, and it projects its installed base will process more than $25 billion in transactions in the course of the next 12 months. Some 8,000 developers have now written applications for the Poynt device.

And besides Elavon, which came on board last year, several more banks and processors have signed on to support Poynt over the years, including Evertec, Worldpay, JPMorgan Chase, Itau Unibanco, Alipay, Nexi, EVO, and Mashreq Bank.

But the company leaves no doubt its major thrust will be to create a unified operating system for the burgeoning market for smart POS devices. The common OS, it says, will drive up efficiency by allowing apps to run on any device.

"Smart phones changed the way we search, buy, and communicate—not only because the hardware was beautiful, but because iOS and Android transformed a ubiquitous utility into a platform for innovation where developers could build once and distribute everywhere," said Osama Bedier, Poynt's founder and chief executive, in a statement. "Our vision is to transform retail by becoming that innovation platform for payment terminals everywhere."

Don't look for this vision to materialize any time soon, some observers caution. They point to a payments world that now includes competing devices from the likes of Square Inc., First Data Corp. (Clover), Verifone Systems Inc., and North American Bancard LLC.

"It's a long way from developing a standard to ubiquity," says Thad Peterson, a senior analyst at Aite Group LLC, a Boston-based research firm, in an email message. "The legacy players are already populating their ... payment systems with apps that enhance the functionality of the terminal, like Clover from First Data."

But by creating an OS that works across a spectrum of smart devices, Poynt just might lock in the relevance of its app store for outside developers. "Developers need to focus on the operating systems that can provide the most downloads," says Rick Oglesby, principal at AZPayments Group in Mesa, Ariz. "That normally means the ones that attract the most eyeballs. If Poynt's OS is tied only to its hardware, the eyeball exposures are more limited, so this is a very smart move."

Even so, while he agrees that "an open system in POS would make a great deal of sense" and "may well be the future of POS," Peterson argues that "it's going to take a long time before critical mass is sufficient to drive adoption of an open OS by competitors."

—*John Stewart*

Shades of Amazon: 7-Eleven Brings Mobile Checkout to the C-Store

Starting last month, consumers shopping at 14 7-Eleven Inc. stores in the Dallas area began trying out the convenience-store chain's new Scan & Pay feature to make purchases without stopping at the checkout counter.

The service, part of the 7-Eleven app that also houses the 7Rewards loyalty feature, enables consumers to avoid long checkout lines, 7-Eleven says. Scan & Pay is available for iOS and Android devices and can pay for all 7-Eleven merchandise except items requiring cashier help, such as hot food, alcohol and tobacco, and lottery tickets.

7-Eleven says consumers can use Apple Pay, Google Pay, or a credit or debit card to pay for items. Purchased items are placed in clear shopping bags. Users also must be in or around one of the 14 test stores for the shopping feature to appear in the app.

Upon completing their shopping, users scan a quick-response code

displayed on the final confirmation screen at a Scan & Pay station.

"Customers can now take control of their shopping experience and earn loyalty points at the same time," Gurmeet Singh, 7-Eleven chief digital officer and chief information officer, said in a press release. "We are taking the in-store retail experience to the next level with a series of innovations. Scan & Pay is one of them."

7-Eleven says it plans to expand the availability of the proprietary payment technology to more cities in 2019.

Scan & Pay, because it's coupled to the c-store chain's loyalty program within one app, is another example of how retailers "increasingly view their app as a platform where they can intertwine payment, rewards, loyalty, and engagement into a tightly integrated and controlled experience," says Jordan McKee, research director at New York City-based 451 Research.

Still, that tight integration likely will be most valuable to a minority of shoppers. "It's unrealistic to think that every shopper will use a retailer's app," McKee says. "Retail-branded apps will only see adoption by frequent shoppers that have a pre-existing affinity for shopping with that specific retailer."

Nonetheless, the effort to produce an app with multiple features could be worthwhile.

"Convenience is a top vertical for implementing a 'grab and go' payment experience thanks to the frequency of purchase, small basket sizes, and limited inventory," McKee says. "7-Eleven's move toward this type of shopping experience is a clear indicator that it sees Amazon Go as a long-term competitive threat."

Amazon.com Inc. this year opened the first of its Amazon Go convenience stores outside of Seattle with plans to add more.

Retailers miss out on a lot of sales—$37.7 billion in the past year according to 451 Research—because of shoppers abandoning long lines, McKee says. "A 'grab-and-go'

payment experience is positioned as an attractive way to help retailers in certain verticals reclaim these missed revenue opportunities."

—Kevin Woodward

If Only Mobile Wallets Functioned More Like Leather Wallets...

Ever since mobile payments first captured the public imagination four years ago with the launch of Apple Inc.'s Apple Pay, experts have debated why usage of the iOS and Android wallets has fallen short of the original, lofty expectations.

Some speculate that usage would rise markedly if the mobile wallets functioned more like their leather counterparts, only with the twist of digital convenience.

And now evidence is emerging to support that claim.

In October, Apple said students at three universities could load their student IDs into Apple Pay, allowing them to use the credential for such routine tasks as going to the gym, opening dorm rooms, or checking out library materials.

Also in October, Ant Financial Services Group's Alipay wallet started supporting marriage certificates in Jiangsu province in China, easing the way for users to apply for a mortgage, transfer property, or open a startup company.

These moves could pay off handsomely for Apple and Alipay, according to research results released last month by Auriemma Consulting Group. In the latest edition of the firm's quarterly Mobile Pay Tracker, more than one-third of mobile-payment users Auriemma surveyed said they'd be interested in using a mobile wallet to store ID cards or government documents.

The New York City-based consulting firm canvassed 1,518 people who had both a major credit card and an Apple or Android phone capable of mobile payments. Overall, 31% of these consumers had ever used mobile payments, the firm found (the breakdown among brands is 35% for Apple Pay, 28% for Google Pay, and 23% for Samsung Pay).

Auriemma's analysts say the convenience of storing digital versions of documents people might otherwise stuff into a leather wallet or store in a safe could pump up mobile-wallet usage.

"We've been doing this survey since Apple Pay launched, and usage

They Like P2P

Apple Pay users who have used Apple Pay Cash

- Q1 2018: 16%
- Q3 2018: 42%
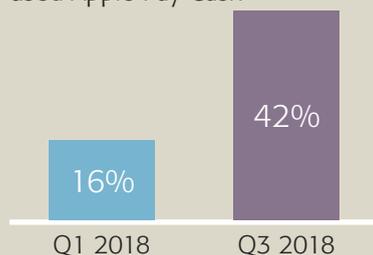
Google Pay users who have used Google Pay Send

- Q1 2018: 25%
- Q3 2018: 36%
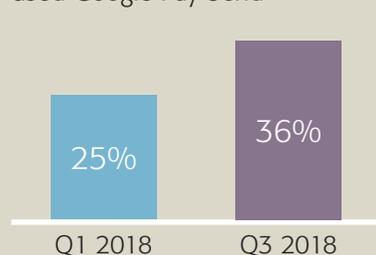
Source: Auriemma Consulting Group

among those eligible to use hasn't seen any spikes," says Jaclyn Holmes, director of the firm's payment insights practice. "Without additional functionality built in, the sentiment we're seeing is, 'we see no use for [mobile payments].'"

Still, peer-to-peer payments on the major wallets appear to be gaining popularity. Apple Pay Cash, in particular, has been catching on fast since its launch a year ago (chart, page 9).

The P2P apps also engender higher spending. For the two services combined, users had sent $162 on average in the past week. By contrast, the average spend in store was $145; on a Web site, $142; and in-app, $133. Ironically, Alphabet Inc. said in July it plans to phase out Google Pay Send in favor of a new P2P service.

—*John Stewart*

An Industry Group Takes on Faster Payments

Following through on plans disclosed earlier this year, the Federal Reserve in November formally unveiled the U.S. Faster Payments Council, an industry group charged with collaborating to spur the adoption of faster payments and identify market opportunities.

The 22 inaugural members range from retailing giant Walmart Inc. to Visa Inc. and Mastercard Inc. to some big banks, tech companies, processors, and automated clearing house governing body NACHA.

The council, an outgrowth of the Fed's multiyear Payment System Improvement project and the successor to that project's Governance Framework Formation Team, will focus on private-sector approaches "to solving problems and addressing issues that inhibit adoption of faster payments," the Fed said in a news release.

The group's first major tasks include a membership drive and recruitment of an executive to lead it.

Duties for the next two years include support for adoption of practices that enhance payment safety; development of an education and awareness program about faster payments, and "identifying, developing and supporting principles, guidelines, and market practices that will address opportunities and emerging issues in an open and collaborative way," the Fed said.

Council decisions will not be binding on members, according to the Fed.

The group is open to any payments-industry company or organization that pays a revenue-based annual fee. Nine fee tiers for voting members range from $500 for firms with less than $5 million in annual revenue to $90,000 for those with revenues above $20 billion.

So-called founding sponsors pay anywhere from $25,000 to $162,000, which includes up to five years of prepaid dues if they pay by Feb. 28, 2019. The annual fee for non-voting associate members is $250.

"We want to have an inclusive approach that brings everybody that has an interest in this space together," Reed Luhtanen, Walmart's senior director of payments strategy, said in October while previewing the council at a Fed conference in Chicago.

The council's board of directors will have up to 21 voting members, with three seats each for financial institutions, payment networks, tech providers, business end users, and consumer groups. Three seats will be reserved for other organizations, and there will be three at-large seats. **DT**

—*Jim Daly*

MONTHLY MERCHANT METRIC

Growth in Same-Store Sales Year Over Year

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

5.77%

5.03%

7.08%

7.01%

7.00%

| Q2 2017 | Q3 2017 | Q4 2017 | Q1 2018 | Q2 2018 |

Note: This is sourced from The Strawhecker Group's merchant datawarehouse of over 3 million merchants in the U.S. market. The ability to understand this data is important as SMB merchants and the payments providers that serve them are key drivers of the economy.

All data is for SMB merchants defined as merchants with less than $5 million in annual card volume.
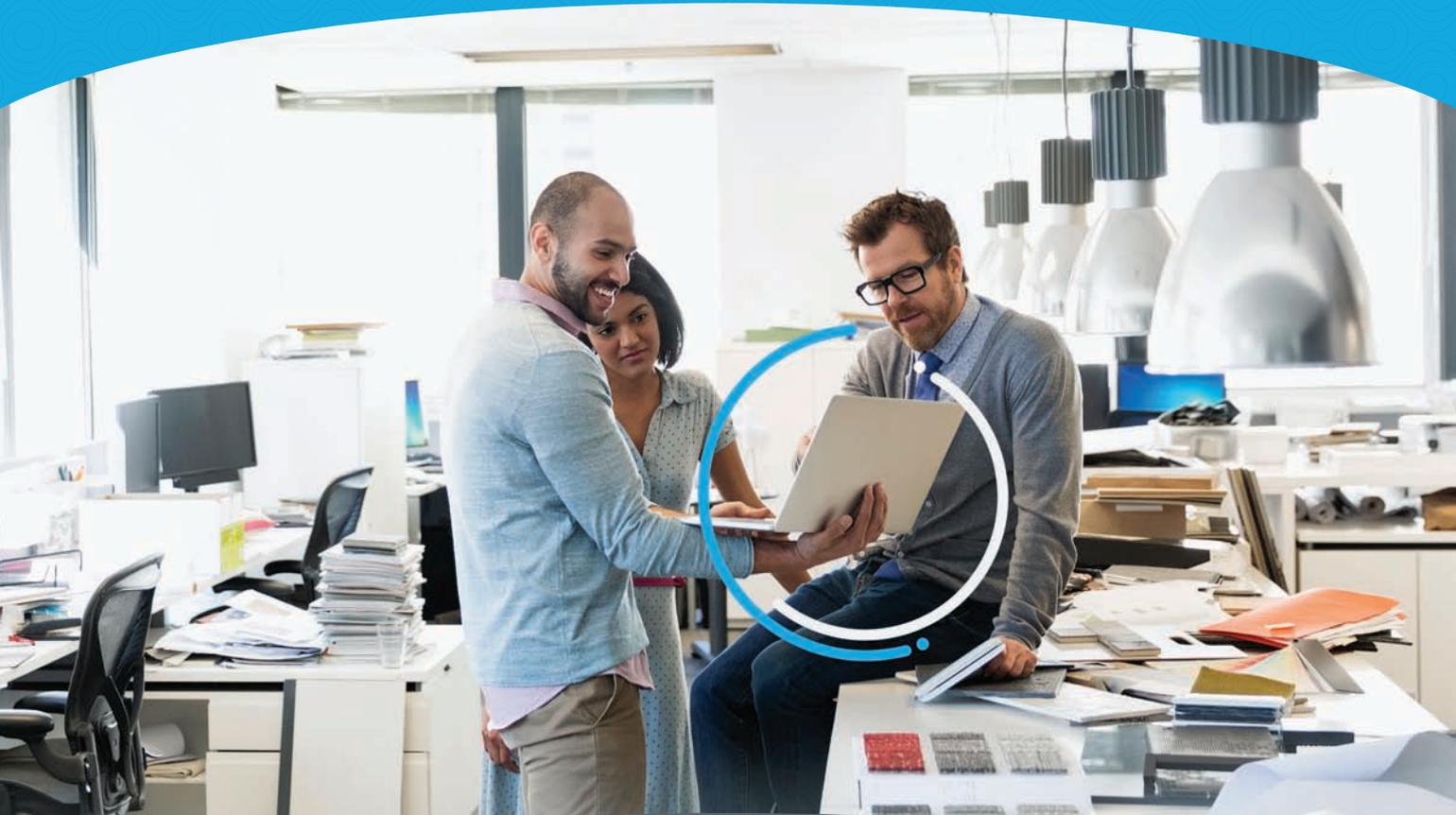
Payments in the Cloud

Gideon Samid • *Gideon@BitMint.com*

I have found out that many payments professionals, who claim to use and comprehend the cloud, view it simply as a remote repository of accounts. So this month I have decided to dedicate this column to one purpose: elucidating this remarkable technology as a service to my readers.

Early in my life in Israel, I lived in a "kibbutz." There were no private cars, but there was a fleet of vehicles ranging from small sedans to large pickup trucks. Members checked out what they needed at the moment. In this way, we achieved effective mobility at a fraction of the "car parked in every garage" cost. Maintenance was centralized and professional. Also, a personal vehicle is often too small or too big for the current purpose.

These savings and efficiencies can be likened to what cloud technology offers its users.

Suppose you have a grand idea for loyalty payments, so you set up a database to manage it. Your idea catches on, and more and more customers log in. Now you have maxed out your server. Response is getting slow, customers drop off. Not good. If instead you contract a cloud provider to host your data, then expansion is seamless and painless. You pay more, but in proportion to your usage requirements. You can start small, but if you become an overnight success, your database resources expand accordingly.

The idea is that you are excused from the need to pre-estimate your capacity requirements. The cloud provider stays ready to accommodate your overnight growth. This is a big help for any payments startup counting its pennies.

The cloud operates with its client via an interface. The client requests database services and receives them. It is important to understand that this communication between the cloud and its client takes place through a veil. This means that you, as the client, are clueless as to the mode, configuration, and location of your data. This remains the domain of the cloud. It takes your data and organizes it as it sees fit.

When you query your database, or change some entries there, you pass the request to the cloud and the cloud takes care of it—again through a veil. You get proper responses, but you are not privy to the particulars of the data handling. That means you are not responsible for that configuration. It is what the cloud does professionally.

You are also relieved of worries about a breakdown. A professional cloud is built with massive redundancy. If some hardware burns out, or some miswiring takes place, there is enough backup machinery to keep your services running. It is all built into the fee, which is usage-determined.

Payment innovators who understand the fundamental advantage of cloud configurations are signing up in droves. Then, when I tell them that their customers' data is exposed to any credentialed employee at the cloud company, they are shocked. Alas, that is the price of convenience.

Also, while clouds are highly resistant to hacking and malfunctions, they are not foolproof. The cloud is not the Federal Deposit Insurance Corp. Its responsibility is linked to the data per se, not the money that is reflected in your database.

The big commercial clouds accumulate so much experience and improve so fast that no private alternative can compete. Much as the Internet, as it grew, killed most private networks, so it is with cloud technology.

Even highly secretive government agencies use commercial clouds, but with "before-and-after" encryption. This means the data is encrypted before it is passed to the cloud, and decrypted after it is returned from the cloud. A powerful new technology called homomorphic encryption enables this protection, which denies the cloud access to private data while enabling the cloud's sorting and selecting capabilities.

Payments are so essential to civil order that it is important to understand how the growing dependency on wireless connectivity makes the cloud a juicy target for hostile agents and places it at risk during natural catastrophes. Serious payments planners ensure continuity by keeping money hosted in phones and other personal devices. Such personally-hosted funds can transact between two battery-operated devices when the Internet is down.

For example, BitMint developed a dedicated money language to accommodate a seamless shift from network-enabled payment to network-disabled payment. For the country that is most advanced in that regard, look at the Peoples Republic of China. ∎

POS Terminal?
What's That?

Kevin Woodward

Cloud connectivity, apps, and features beyond payments are shaping the next evolution of the point-of-sale terminal.

With all the discussion surrounding merchant adoption of point-of-sale systems and integrated payments, one might think the days of the conventional POS terminal are numbered. Their days as an isolated piece of equipment with a sole function as the entry point for payment transactions may be dwindling. But, that does not mean the venerable POS terminal is about to become an historical artifact, as long as it's not in isolation.

"Any system today, whether it's a point-of-sale or hardware device, that is not cloud-based is dying," proclaims Jared Drieling, senior director of business intelligence at The Strawhecker Group, an Omaha, Neb.-based payments advisory firm.

Today, a conventional POS terminal may still sit on the countertop, but with increasing likelihood it's connected to POS software. It still captures payment data, but now it may act as the citadel, protecting the integrity of the data and sharing only the minimum information necessary with the software. The POS terminal may have a PIN pad or signature-capture capability. It may enable consumers to enter loyalty-program information or redeem offers.

In instances where there is no conventional POS terminal, a merchant likely has a tablet-based POS system in place. Since 2010, when Apple Inc. debuted its iPad and POS software developers flocked to the form factor, tablet-based POS systems have steadily gained favor among merchants.

'Very Limited' Growth

At first, the tablet form factor, like the smart phone before it, was innovative and attracted businesses. Then, as cloud connectivity improved, the opportunity developed to bundle other services, such as employee scheduling, inventory management, pricing, and detailed sales reports, making cloud-based POS systems the preference for many businesses, especially small businesses that now could afford them and had a need for them.

That has had a dramatic effect on the market.

Even traditional POS systems, which typically had updates performed when the maker sent a technician to install new software or hardware, are losing ground against cloud-based systems, Drieling says. Some merchants avoided these updates because they might cost thousands of dollars.

"In legacy systems [POS system makers] developed the code and would try to customize it for you," Drieling says. "Cloud-based POS systems can be integrated with new or existing systems. It allows the developer to integrate other software into that system without having to create software to bridge the two together."

Such developments mean that the outlook for conventional POS terminals is quickly changing. "Conventional countertop devices are going to be around for a very long time, but the growth of that category is very, very limited," says Thad Peterson, senior analyst at Boston-based Aite Group LLC.

That's because a dedicated POS and payment device isn't as useful or cost-effective as an integrated platform like, for example, Square, he says. Square Inc. introduced a magnetic-stripe-only card reader in 2009, but followed up with POS software for the iPad, and now, interestingly, offers its own Square Terminal for $399.

'Reactionary Mode'

For sure, Square is one of many to launch so-called smart terminals, which use apps and enable easy integration to POS software. Square chief executive Jack Dorsey even heralded the new Square Terminal during a November earnings call as the replacement for "dinosaur" POS devices. The same month, payments provider North American Bancard Holdings LLC launched its own smart terminal, joining competitor Poynt Co., which debuted its device in 2014. (For more on Poynt, see p. 7.)

Co-Branded E-Mail Marketing

Get the Results You Need

Here's how it works:

You select the part of *Digital Transactions'* subscribers you want to reach, sorted how you need it, by function, location, or title. Just ISOs? No problem. Just executives on the East Coast? No sweat. Just CEOs? No worries. Or choose our entire circulation base. It's up to you!

You give us your HTML creative.

We create both a text version and a Web version of the e-mail deployment.

After the deployment, we track deliveries, opens and clicks, and give you all the stats.

It's really that easy!

To get started, contact Publisher Bob Jenisch today:

877-658-0418
bob@digitaltransactions.net

Verifone's Carbon line of smart terminals targets small and medium-size businesses.

(Photo: Verifone Systems Inc.)

The common denominator in all these devices is the connectivity. That is a boon to small businesses, which had to forgo POS systems of the past because of the costs. "The most critical point to why these cloud-based systems are growing, primarily in the small and mid-size space, is they allow a lot of integration," Drieling says.

This ability to integrate payments with software that can run other business functions is much sought-after in retail. In August, for example, payments provider Global Payments Inc. paid $700 million for AdvancedMD, developer of medical-office management software.

This all points to a very cloudy future. For the likes of Verifone Systems Inc., Ingenico Group, and Equinox Payments, which sprang from the former Hypercom Corp.'s U.S. unit, their roles as providers of traditional POS terminals will change, Peterson says.

"The challenge with the Ingenicos and Verifones of the world is they are in reactionary mode," he says. "But they're easily disrupted by players coming in with more flexible and lower-cost offerings."

Going Up Market

It's not for lack of effort on their part. San Jose, Calif.-based Verifone,

which went private this fall, has been emphasizing services revenue for years and launched its Carbon line of smart terminals to better compete.

Paris-based Ingenico, too, has grown its services revenue and made changes. In April, it launched the Moby/C150 ECR that features an Android-based tablet with a 15.6-inch display.

As it adapts to changes among merchants and consumers, Ingenico finds itself examining the point of interaction between consumers and merchants. While Mark Bunney, Ingenico North America director of go-to-market strategy, says there will still be customers for standalone POS terminals, the market is changing.

"Lots of the tablet or mobile POS providers are definitely changing some of the dynamics in the marketplace," says Bunney. "We have to change not only from a hardware perspective, but [in] how it's going to impact our software and services."

Bunney points to Apple's own retail stores and Amazon.com Inc.'s Amazon Go locations as examples of this change. There is no POS station in an Apple store. It's all mobile, Bunney says. And in Amazon Go stores, the consumer's own smart phone with the Amazon app is the payment mechanism.

Square Terminal: Square's latest POS device.
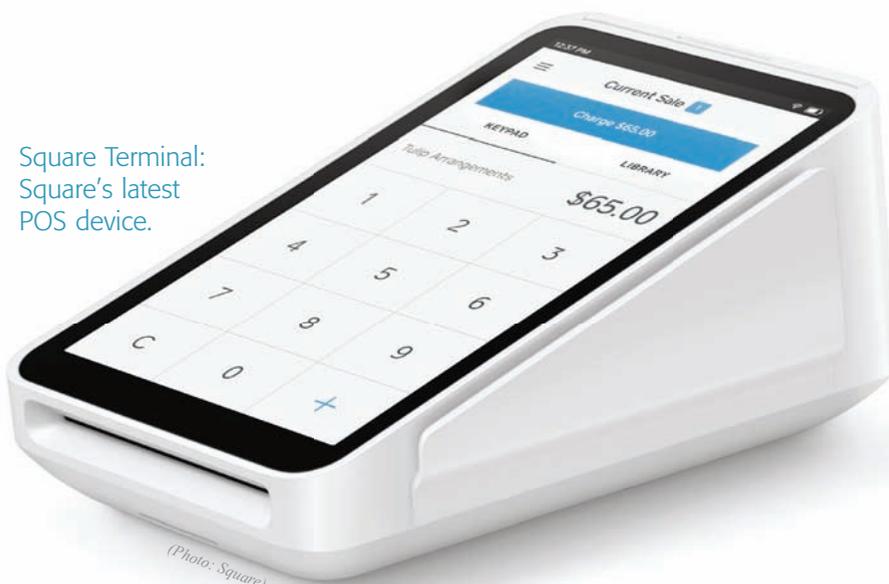
(Photo: Square)

Of the three primary categories of POS-terminal technology—the standalone device, the integrated POS, and mobile POS—demand for standalone devices is declining, Bunney says.

"That's part of the market migrating to an integrated solution or going to a more tablet solution," he says. "The other thing we're seeing in the integrated market is merchants as well as the consumer want to have additional interaction beyond just the payment with the merchant."

That mirrors what Peterson sees in the market. "The customer experience used to be managed by the merchant," Peterson says. "Now, the consumer controls their own experience."

That control has been enabled by the versatile tablet. "Now, the POS could look like a tablet," Bunney says. It depends on the type of interaction consumers want, he says. "People want sleeker-looking solutions," he says. "They don't always necessarily want to have a separate payment device from the tablet."

That's not to say that a tablet, or cloud-based POS system, is for every type of merchant. Bunney doesn't think large merchants would be as satisfied with a tablet-centered POS as they would be with something designed for their complex needs.

Still, some cloud-based POS system providers have made moves to go up market. Square Terminal, with its integration capability, is one example, and First Data Corp. is promoting its Clover POS system for fine dining.

Postponing Extinction

How the POS experience will adapt is uncertain, with its dependence on how consumers shop and the technology they use and how merchants react to these changes.

However it evolves, there will be integration of the payment-acceptance device into the overall checkout experience.
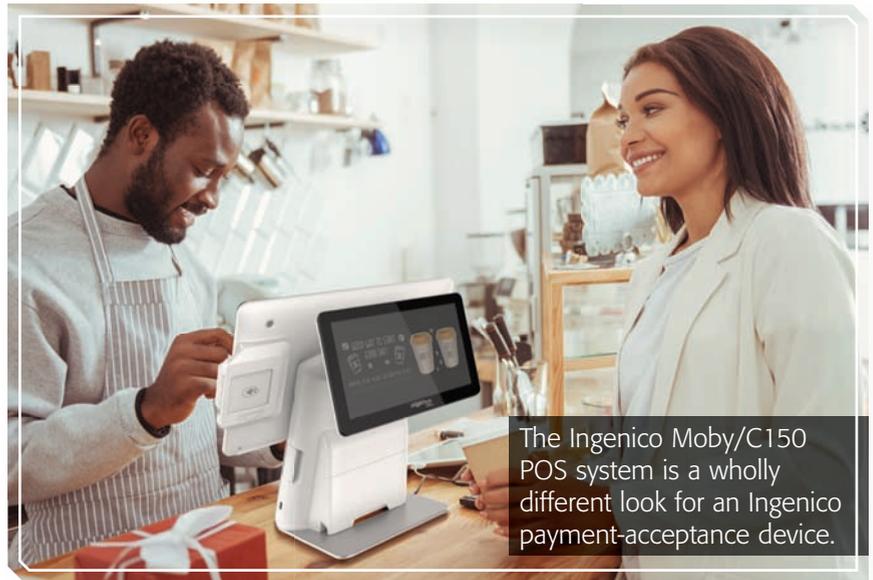
The Ingenico Moby/C150 POS system is a wholly different look for an Ingenico payment-acceptance device.

(Photo: Ingenico)

"The standalone device where it's not talking to the POS is in decline," Bunney says. Yet he doubts it will disappear completely, despite Square's claim the older tech is a "dinosaur." "In some areas, it may not be growing at as fast a rate," he says. "There is still that interest level."

The hardware side may not change too much in the near future, Bunney says, with the exception of some devices, like tablets, gaining contactless-payment acceptance. Most POS terminals shipped since at least 2015 by the likes of Verifone, Ingenico, and Equinox have contactless tech built in, if not yet activated.

Better contactless identification marks may be part of future devices, Bunney suggests. "How do you make it easier for the consumer to interact from a hardware perspective?" he asks.

POS software, in all forms, will evolve much faster, he says. Not only will industry standards from EMVCo, which sets the specifications for EMV chip-card acceptance, influence this, so will PCI Security Standards Council standards on PIN-on-mobile, which enables commercially available devices to securely accept PINs.

PIN-on-mobile is one of the trends Peterson sees influencing the evolution of the POS experience. It's devolving the POS into smart devices that are not POS devices, he says. More use of mobile devices, especially for in-aisle checkout, and increasing awareness and availability of alternative payment methods are two other trends.

The Ultimate Payment

The so-called traditional POS makers will have to evolve, says Drieling. "They need to come out with some competitive products," he says. "They know the POS industry very well. They probably have the capability to bring out some competitive cloud-based POS products. I don't see them doing very much in the independent software vendor space."

ISVs increasingly look for a partner to handle the payments element, alleviating much of the issue surrounding payment-device certification with their software.

The future POS may not even resemble a POS device or tablet.

Even Amazon's Alexa voice assistant almost qualifies as a POS device, Drieling says. Echo and other in-home devices enable consumers to use their voice to authorize orders. "The next step is unified commerce," he says, allowing a consumer to start a transaction in one channel and go through others until making the ultimate payment. **DT**

BATTLING THE BOTS

There are plenty of good bots out there, but the bad ones are making life difficult for financial institutions and merchants. And it's only getting worse. What's to be done?

BY JIM DALY

To paraphrase Glinda, the good witch in L. Frank Baum's Oz novels and the 1939 film *The Wizard of Oz:* **Are you a good bot or a bad bot?**

There are plenty of good bots out there that perform useful tasks in the Internet age. They're bits of software code, artificial intelligence really, that are programmed to react to human inputs—typed messages or voice commands—and react fast with information or advice ("The Age of Bots," January, 2017). An example is an automated assistant that facilitates e-commerce purchases.

The trouble for merchants, banks, and the payments industry is there are too many bad bots—malicious software applications designed to run repeated code on their own. They can unleash massive attacks on the login pages of retailers, banks, and credit unions, or any organization with personal or financial data accessible through the Internet.

"With bots, they get all of these credentials from data breaches, and they just hammer until they find one that matches," says Shirley Inscoe, senior analyst at Boston-based research and consulting firm Aite Group LLC.

Account takeovers, a type of fraud in which a criminal gains control of a legitimate credit card, bank, or other type of financial account, are a frequent result of successful bot attacks.

Bad bots can pull data from a database, for example, a retailer's customer list with valid passwords and usernames, and, in a type of attack dubbed credential stuffing, attempt to get into a consumer's online account without much operator action.

A SWELLING STREAM

Bots typically run from servers, while some attacks rely on connected computers or Internet of Things devices surreptitiously recruited into the attacking swarm, or botnet.

These botnet attacks are generating a swelling stream of new business for a small army of specialist vendors with anti-bot technology. And most informed observers agree the scale of bot attacks is huge.

Ninety percent of login attempts may now be using bots, estimates Colin Sims, chief financial officer at New York City-based fraud-prevention firm Forter Inc. "One of the ways you try to brute-force your way into an account is using a bot," he says.

The attacks are only growing more numerous. In both May and June there were 8.3 billion malicious login attempts by bots, according to Akamai Technologies, a Cambridge, Mass.-based Web-services company.

In the eight months from November 2017 through June, Akamai tracked more than 30 billion malicious login attempts, says the company's 2018 State of the Internet report released in September.

Only a relative few of the bot attacks actually breach the defenders' electronic walls, tech executives say, but more are succeeding.

Based on a late-2017 survey of more than 5,000 U.S. adults about their experiences with identity fraud, Javelin Strategy & Research estimates that account takeovers tripled over the preceding year to hit a four-year high. The Pleasanton, Calif.-based firm estimates losses reached $5.1 billion.

Bombarded by Bots

8.3 billion
There were 8.3 billion malicious login attempts in May and an equal number in June.

3x
Account takeovers, often linked to bots, tripled in 2017.

$5.1 billion
Account-takeover losses hit $5.1 billion.

89%
89% of financial-institution executives say account takeovers are a top-three cause of fraud losses.

Sources: Akamai Technologies, Javelin Strategy & Research, Aite Group

LIKE GOING TO THE BANK

Bot-deploying criminals are devoting plenty of attention nowadays to retailer Web sites, which tend to have weaker defenses and are subject to fewer data-protection regulations than banks and credit unions, security experts say. Plus, fraudsters try to take advantage of the proclivity of consumers to use the same passwords across multiple sites.

"It's something [retailers] haven't dealt with before," says Al Pascual, senior vice president of research and head of fraud and security at Javelin. "For criminals, this is almost as good as going to the bank."

While retailers are popular targets nowadays, there are many other ones, including health-insurance providers, and the more skilled fraudsters continue to probe banks for weaknesses.

"We are seeing a massive number of account-takeover attempts," says Robert Capps, vice president and

authentication strategist at NuData Security, a Vancouver, British Columbia-based antifraud specialist owned by Mastercard Inc. that uses behavioral biometrics to spot suspicious activity. "We see a lot around retail, we see a lot around payment services. We're seeing this drumbeat pretty much around anyone who has value behind that login."

In an October report about data protection, Aite said 89% of financial-institution executives it surveyed stated that account takeover is a top-three cause of fraud losses in digital channels, and 42% said application fraud also is a top-three source of losses (see the Endpoint column on page 30 for more about account-takeover fraud).

'UNSATISFIED CUSTOMERS'

Even if they're not causing actual fraud, bot attacks can wreak mayhem because of the sheer volume of traffic directed at target Web sites.

'We are seeing a massive number of account-takeover attempts.'

—ROBERT CAPPS, VICE PRESIDENT AND AUTHENTICATION STRATEGIST, NUDATA SECURITY

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

The traffic can resemble a digital denial of service (DDoS) attack, in which the goal is not so much to steal as to disrupt by causing a site to slow down or crash, leading to "unsatisfied customers," says Rich Bolstridge, chief strategist at Akamai Technologies.

"The botnets keep trying and trying," he says.

One retailer client of Cequence Security was hit with a 10-fold increase in Web traffic, 90% of it malicious, when it ran a sale over the Memorial Day weekend, notes Larry Link, president and chief executive of the Sunnyvale, Calif.-based fraud-control technology firm.

"I was surprised at the level of sophistication that hit them," Link says. "It's anybody that's got a big retail presence."

Link adds that another weak spot bots try to exploit involves application programming interfaces (APIs), the communication protocols and tools developers use in creating their programs. APIs help outside software developers work with a particular program, but they're often vulnerable from a security standpoint, he says.

'THAT'S A PROBLEM'

Thwarting malicious bots could soon become harder because of the rise of so-called open banking in parts of the world, including the European Union, according to Bolstridge. Open banking refers to regulations that allow financial-technology firms to access some of the customer payment data held by banks.

The intent is to enable fintechs to offer a broader array of services to consumers. But these intermediaries now represent a new group of targets for criminals.

"It's going to make [fraud control] even more challenging," Bolstridge says.

What to do?

Fallback Fraud Falls

While merchants and financial institutions are fighting a pitched battle against bots, they are winning in another arena of fraud. Fallback fraud, an offshoot of the counterfeit fraud that EMV chip cards are meant to reduce, declined over the past year, according to new findings from Auriemma Consulting Group.

Fallback fraud refers to dollar losses resulting from would-be EMV payments resorting to the credit or debit card's back-up magnetic stripe because of a problem with the chip. Such transactions typically occur when the fraudster damages the chip, covers it with clear film, or otherwise renders it inoperable.

That forces the point-of-sale terminal to read the card's mag stripe, which likely has been counterfeited. Incorrect insertion of an EMV card into a POS terminal occasionally initiates a fallback transaction, too.

In 2017, fallback fraud made up more than 20% of counterfeit fraud and 4.5% of total credit card fraud, according New York City-based ACG's Card Fraud Control Benchmark Study released in November. Fraud was rising even as fallback transactions, including legitimate transactions, made up less than 2% of overall purchase authorizations, ACG reports.

But in 2018's second quarter, fallback fraud made up just 11.5% of counterfeit fraud and 3.2% of total credit card fraud, respective declines of 45% and 30% year-over-year, according to ACG.

Auriemma gets its data from its quarterly Fraud Control Roundtables with representatives of 34 financial institutions, including 14 of the 15 largest U.S. credit card issuers, says Ira Goldman, senior director of the Roundtables operation. The firm also collects fraud data from issuers through monthly and quarterly surveys.

Fallback fraud is an activity that typically comes and goes fairly quickly after a nation converts to EMV chip card payments, though it has stuck around longer than usual in the United States, ACG said. But issuers are getting smarter about identifying and thwarting it, according to Goldman.

"They're looking at dollar amounts, they're looking at velocity thresholds [the number of transactions in a given time period], any sort of prior fallback activity on the same account," Goldman says.

Fraudsters often try to get the most bang for their buck by trying to buy TVs and other pricey consumer electronics goods, thus issuers' increased emphasis on dollar limits on fallback transactions. "The fraudster is looking to purchase an expensive item," says Goldman.

Issuers also are looking more closely at fallback history as they try to sort the good from the bad. "There are legitimate fallback transactions," he notes.

Banks that have implemented new fallback-fraud policies are reporting minimal disruption to customers, according to Auriemma. Fallback transactions and declines fell 12.6% and 20% year-over-year, respectively, the firm reported.

Merchants, banks, credit card issuers, insurance companies, and others increasingly are looking to tech firms to help sort out bad bots from legitimate traffic, all the while trying to minimize the risk of rejecting honest transactions.

One of the anti-bot technologies being brought to the front lines is behavioral biometrics, which involves software programs that can measure hundreds of variables, everything from the strength of the person's keyboard tap to the width of fingertips on a touch screen to typing patterns.

"People, when they enter [data into] a machine, they don't have even typing patterns," says Frances Zelazny, chief strategy and marketing officer of BioCatch, a 5-year-old firm based in New York City that monitors six

billion transactions per month, including banking and credit card applications. Bot-supplied data "is going to look like a machine, but a human will have many, many different nuances."

Zelazny describes one trick BioCatch has used to thwart bot-driven credit card applications. Banks, card issuers, and others that need a customer's birth date often display "wheels" containing days, months, and years from which the applicant is supposed to select his or her birthday. BioCatch's technology can make the wheels spin faster or slower, a move that humans adjust to much easier than bots, Zelazny says.

"They weren't able to react, they expect the wheel at a certain speed," he says.

Bots have improved over the years, data-security executives admit, but they still often betray themselves with robotic behavior, however subtle.

"If all those touches are uniform, they're all the same size, that might be automation," says NuData's Capps. "If something's too perfect, that's a problem. If something's too random, that's a problem."

Adds Zelazny: "There are certainly bots that are trying to behave like humans, but they can't react because they're scripts."

'LOW AND SLOW'

Despite their scripted behavior, some bots have their own tricks, and these can help them evade attention. One is to slow down their normally very high rates of login attempts.

In a recent report about credential stuffing, Akamai describes the unpleasant situation a large credit union found itself in: Under attack by three separate botnets at once.

The first sign of trouble was a more than tenfold increase in malicious log-in attempts per hour, from about 800 under normal conditions to a spike of 8,723. But Akamai calls the botnet responsible for this attack "dumb" because all of its traffic came from two Internet Protocol (IP) addresses based on a cloud platform, and for other characteristics.

The second "bot herder," as Akamai's report calls it, "was impatient and attacked at such a high rate it couldn't escape notice." Over the course of three days, this botnet generated more 190,000 malicious login attempts from thousands of IP addresses. This one needed more work to defuse than the first.

But the third bot proved to be the most dangerous and difficult to detect. "This bot used a 'low-and-slow' approach to attacking the site, averaging one malicious login attempt every other minute," the report says. It used 1,500 IP addresses, but the average of login attempts per address over the time of the attack was very low.

This third, more subtle attack "does highlight the increased sophistication of the botnets," says Bolstridge.

Another technique gaining favor among account-takeover fraudsters is to lie low after capturing an account, according to Forter's Sims. As an example, why use credentials good for a relatively low-ticket food-delivery service if, with a little time and effort, you find out those credentials also work at a high-end retailer?

"A popular one today: take over the account and not transact because they're trying to get other data points because they want to take the information to commit a bigger type of theft," Sims says.

'SINKHOLING'

It's attacks like these that are prompting data-security vendors to roll out new anti-bot products. One of the most recent comes from Cequence, which in November unveiled its Cequence ASP, for application security platform.

The platform uses artificial intelligence, machine learning, and other technology to first identify the Web assets that a client needs to protect. It then monitors the client's Web and mobile applications, as well as its APIs, for signs of attack, Cequence CEO Link says.

A point of differentiation for Cequence ASP from older anti-bot technology is its ability to work with clients' existing Web applications, says Link. JavaScript, a popular Web-coding technology, requires code injections and software development kit changes for each Web or mobile application, according to Cequence.

"We do this with absolutely no change to the application environment," Link says.

Another differentiator, Link says, is an open architecture. That means the service can be deployed on-premise or in the cloud, and easily exchange data among other systems and devices.

The service is tailored for very high volumes—it comes with a tiered, subscription-based pricing model starting at $150,000 a year based on analyzing 10 million transactions per day.

Once a botnet is identified, defenders have various options to neutralize the attack. A common one has been "sinkholing" the traffic, where it's re-routed to a so-called negative address where the bot's credentials can't be tested. Such an address is one "where's there's basically nothing," says Javelin's Pascual.

'I was surprised at the level of sophistication' of a botnet attack on a retailer.

—LARRY LINK, PRESIDENT AND CHIEF EXECUTIVE, CEQUENCE SECURITY

When the new Cequence ASP confirms a bot attack, the system attempts to squelch it through blocking, limiting traffic, deception, and other techniques. Cequence says it has tested the new service in several deployments, including a Fortune 100 multinational financial-services provider and a Fortune 500 cosmetics retailer.

'RAISING THE BAR'

Apart from using this or that anti-fraud product, merchants, financial institutions and others with data to defend need to take a broader approach to fighting botnets that focuses on more than just transactions, according to Sims at Forter.

"You really need to monitor every stage of the customer lifecycle," he says. "If you just look at the point of the transaction, you're setting yourself up to fail. Avoid the traditional rules-based analyses, try to monitor as many different touch points in the customer lifecycle as possible, not just the checkout."

Good bot defense also goes beyond technology and defense strategy to factor in consumers' perceptions of how well companies guard their data, according to Pascual. That's especially true for retailers, who are newer to the data-protection game than banks.

"If my competitors offer better security ... that could be a competitive advantage," he says. **DT**

—With additional reporting by Kevin Woodward

'You really need to monitor every stage of the customer lifecycle.'

—COLIN SIMS, CHIEF FINANCIAL OFFICER, FORTER INC.

The Promise—And Threat—of Real-Time Payments

John Stewart

Three years ago, Mastercard shelled out big money for a U.K. technology firm. As faster payments take hold in the States, the rationale for that deal will soon be put to the test.

Back in July 2017, the Federal Reserve issued a challenge to the U.S. payments industry: create a nationwide real-time payments regime by 2020. While that challenge set many hands wringing, at least one company figured it was already set up to meet the goal.

In May last year, Mastercard Inc. had closed on its $920 million acquisition of VocaLink Holdings Ltd., a London-based software house renowned for its expertise in real-time transactions. The firm, after all, had built the network for the United Kingdom's Faster Payments Service, which is already a decade old.

By the time it joined Mastercard, VocaLink had already gone to work on a real-time switch for The Clearing House, the New York City-based bank processor owned by 25 U.S. financial institutions, including the nation's money-center banks. That technology went live in November 2017, processing transactions in mere seconds.

But the TCH system involves more than just fast clearing and settlement. It also includes some extra twists that could prove crucial for a wide range of applications now served by card and automated clearing house rails. By design, the system can handle data payloads as it transmits requests for payment and requests for information between parties.

That extra transmission channel may sound mundane. To TCH, it's anything but. "We're catching up, but in a lot of ways we're leading the rest of the world," says Irfan Ahmad, a former health-care expert who is senior vice president for product development at TCH.

Largely because of VocaLink's work with TCH, real-time business-to-business and business-to-consumer volume in the United States will hit $849 billion by that crucial year, 2020, nine times the volume in 2017, according to projections by Mercator Advisory Group (chart, page 29).

Real-Time Chops

For Mastercard, however, VocaLink's real-time payment chops are important for reasons that go beyond meeting a Fed deadline. Indeed, the rationale may well go beyond its acquisition of a key position in faster-payments development not just in the U.S. but in other parts of the world where VocaLink is active, including Singapore and Thailand.

With this deal, Mastercard has bought insurance against a future in which card payments may not figure so prominently as they do now. "In the past, whatever the problem was, the answer was always a card," says James Anderson, the company's executive vice president of commercial products.

With faster—especially real-time—payments, that outlook had to change, Anderson says. "One threat [Mastercard analysts] identified was real-time payments," he says. That's because what VocaLink and others offered was faster payments without a card on rails that could conceivably do what card networks do.

At the stroke of a pen, the VocaLink deal "moved [Mastercard] from a card network to a payment-solution provider. That's quite subtle but very powerful," says Dean Wallace, practice lead for real-time and digital payments at ACI Worldwide, itself a developer of real-time payment technology.

Both Mastercard and Visa offer real-time products, but Mastercard Send and Visa Direct depend on card pipes and card rules. Both are derivatives of a protocol called the original credit transaction, which was developed in the first place to get refunds instantly to customers when they returned merchandise they had bought on a card.

"It was a threat if someone developed real-time [capability] that was not on card rails," Anderson says. Hence, it wasn't hard to develop a strong rationale to buy VocaLink, he says.

The payments market is large and fragmented.

DigitalTransactions.net gathers the most important news in one place, and shows you how it all fits together to impact your business.

Concise, clean interface is easy to navigate

Breaking news from the payments market, posted daily

Calendar of industry events

Complete current and past issues of *Digital Transactions* magazine

Detailed listings of payments market suppliers

13 years of payments news and analysis

DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

Also figuring into the deal was the progress Mastercard had already made in bill payments, another prime channel for faster payments. "We had a bill-pay directory. Faster payments comes along and that becomes a strategic asset," he says.

In October, Mastercard announced a service it plans to roll out next year that will rely on TCH's real-time engine to attack a U.S. bill-pay market the card company estimates at 15 billion annual payments totaling $4 trillion in value.

Experts see the new service taking share away from billers and the so-called biller-direct payment channel. "The U.S. is quite unusual in that lots of the billers do it directly themselves. What this is trying to do is be a single interface for all these bills," says Gareth

> 'The U.S. is quite unusual in that lots of the billers do it directly themselves. What this is trying to do is be a single interface.'

Lodge, a U.K.-based senior analyst for payments at the research firm Celent.

Now the question is what else Mastercard can do with its newfound real-time expertise. If the card company really wants to get beyond cards, some observers say there might be an avenue toward merchant acceptance with existing VocaLink technology, though such a move could upset a lucrative, decades-old interchange system.

Observers suggest one way this could unfold is through VocaLink technology called the Pay By Bank app, which enables fast transfers via a mobile-banking app. Designed for online checkouts, the app could be adapted to some physical-world scenarios, these observers say.

"Real-time payments at point of sale are in fact an important part of our VocaLink strategy," says Anderson.

How Faster Payments Are Triggering Opportunity for Merchant Acquirers

When it comes to faster payments, merchants don't want to be left out, and that's creating a big opportunity for payments processors and other acquirers.

Indeed, as the payments industry shifts toward real-time and near-real-time money movement, payment processors can cash in on the value of getting good funds into merchants' accounts instantly, processor executives say.

"Especially in the small- and medium-size business world, they're willing to pay a premium for it," says Henry Helgeson, head of integrated solutions at Columbus, Ga.-based Total System Services Inc. (TSYS).

Paysafe North America, the Shenandoah, Texas-based unit of London-based Paysafe Holdings U.K. Ltd., has come to the same conclusion. In September, it launched a program called "Accelerated Funding" that includes options from next-day to same-day to "Express" funding. The last choice delivers funds within hours to a linked debit card. "There are certain verticals where merchants really need the funding," says Todd Linden, chief executive.

He agrees with Helgeson that demand is coming largely from small and medium-size merchants. Restaurants and bars, in particular, respond well to the idea of getting their funds for Saturday and Sunday sales without having to wait until Monday, he says.

Faster funds can command a premium because they incur higher risk. "We're funding the merchant before

we get paid," says Linden. "So we charge more." Helgeson points out that "there's very little recourse" once the funds are disbursed. At the same time, there's only a matter of hours to vet transactions for fraud. "So there has to be a premium," he adds.

An example of what the market will bear for faster funding is Square Inc.'s 3-year-old Instant Deposit feature, which delivers funds to merchants within seconds for a fee of 1% of the funding amount on top of ordinary transaction fees.

The plan at TSYS is to use its ProPay unit to manage faster funding, Helgeson says. TSYS acquired ProPay, an early entrant in what is now a crowded market for payment facilitators, in 2012.

The pipes will come from Visa Inc. in the form of Visa Direct, a service that transfers money in real time via an original credit transaction, or OCT. The OCT was designed to deliver quick refunds to customers when they return merchandise to stores, but lately it has been harnessed for fast transfers to businesses, as well.

For its real-time funding service, Paysafe is relying on Alpharetta, Ga.-based Ingo Money Inc., whose technology enables push payments between accounts. Linden sees delivering faster funding as a way to get in step with a global trend toward real-time payments.

"It's something we need to do, and we're catching up with the rest of the world," he says. "It seems only fair to give the merchant his money."

How U.S. Faster Payments Will Take off

(Volume in billions for business-to-business and business-to-consumer payments)

■ B2B   ■ B2C   ■ Total

Year	B2C	B2B	Total
2017	$46	$49	$95
2018[1]	$144	$138	$282
2019[1]	$260	$301	$561
2020[1]	$410	$439	$849
2021[1]	$527	$659	$1,186
2022[1]	$632	$956	$1,588
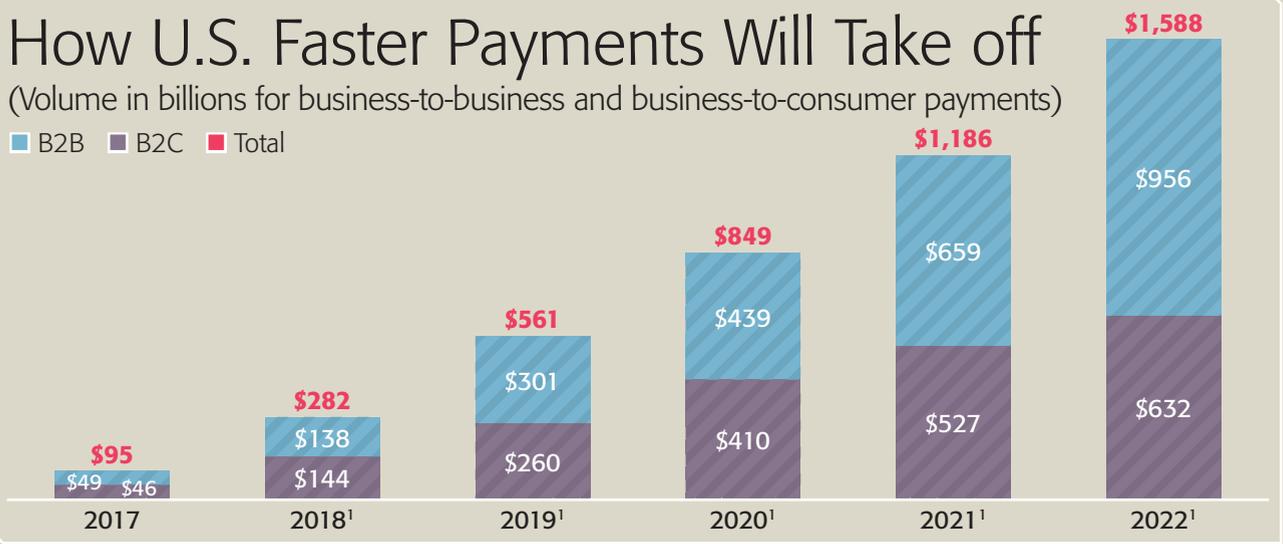
1. Forecast

Source: Mercator Advisory Group

"Following our acquisition of VocaLink, we have increased our focus on innovation around real-time payments globally. In the U.K., Pay by Bank app has been gaining momentum."

Indeed, progress for the app seems strongest at the moment in Britain. Barclays Pingit, a mobile-transfer service, and HSBC are supporting the app or soon will, "and a significant number of the U.K.'s retailers will be offered Pay by Bank app as a new way to pay for their customers," Anderson adds.

'Pole Position'

A wild card for all real-time players surfaced in October when the Federal Reserve indicated it is looking into starting up a service for real-time gross settlements, including a liquidity tool. The banking regulator is taking comments on the idea through Dec. 14, but just the suggestion of its direct entry as a player in a game over which it had been presiding as a sort of umpire has set some observers' teeth on edge.

In the view of some, indeed, the idea of a Fed service may have come at the suggestion of smaller financial institutions that are wary of what they see as big-bank dominance of TCH. "There's an element of truth to [that]," says Eric Grover, a Minden, Nev.-based payments consultant. The Fed, he says, wants "to stay relevant with small banks."

Indeed, small banks may see in a Fed service the sort of competition that could keep TCH from overreaching on price and other terms. Most small institutions are connecting to TCH via core processors rather than directly.

"They feel the Fed represents a choice in real-time payments," says Sarah Grotta, director of the debit advisory service at Mercator Advisory Group, a financial-services consultancy in Maynard, Mass.

A real-time gambit from the Fed could also prove to be a golden ticket for Mastercard. "If the Fed decides to proceed, Mastercard will have an opportunity to bid. They'd almost be in pole position to win this," notes Grover.

'In the Dark'

For now, Anderson is content with what he sees as an unfolding trend Mastercard anticipated back when it made its move to buy VocaLink. That trend, he says, is even bigger than real-time payments.

"What we see that others didn't see is there's a pent-up demand to upgrade the [payments] infrastructure," Anderson says. An opportunity that big, he adds, comes along once in a generation.

Yet, so far, he isn't seeing much reaction out of his rivals at American Express Co., Discover Financial Services Inc., and Visa Inc. "I would be very happy," he says, "for them to wander along in the dark." **DT**

VocaLink's Pay By Bank app: A route to the point of sale?

While companies are hesitant to disrupt consumer convenience, ATO can severely damage brand reputation. When debating between the two, consider the lifetime value of a lost customer.

Balancing Consumer Expectations And Fraud Prevention

Rich Huffman is senior director, product management, at Equifax Inc., Atlanta.

There are no perfect solutions for account-takeover fraud, but tactics such as consumer education and prevention at log-in can make a big difference, says Rich Huffman.

According to Javelin Strategy & Research's report entitled, "2018 Identity Fraud: Fraud Enters a New Era of Complexity," account takeovers (ATOs) tripled in 2017, resulting in $5.1 billion in associated losses. And the losses are more than just monetary. The same report estimates this crime takes, on average, 15 dedicated hours and $290 in out-of-pocket expenses for a victim to resolve. This doesn't even factor in the costs of churn by estimating the average lifetime value of lost customers.

ATO is a criminal's gold mine in more ways than one. This type of fraud offers a lot of information for criminals to use because of the associated account credentials accessed with tactics such as man-in-the-middle (MITM) attacks. An MITM attack occurs when a fraudster either taps into a call between a user and service provider, or impersonates a service provider, to obtain personal information.

Whether it's through MITM or hacking, once criminals have their entry points, they can do more damage through password testing on popular Web sites by trying to find relevant matches. Automation, specifically the use of bots, makes this process even easier.

But with the uptick in ATO comes more options for addressing this challenge. To face the rising incidents of ATOs in today's digital environment, businesses, including retail bankers and processors, must address the issue with knowledge and newer, relevant technologies.

An Enterprise Issue

Gone are the days when fraud was finite. According to the National Institute for Technology Standards (NIST), using SMS or email for out-of-band or multifactor authentication is no longer secure. Reliance on passwords and "what-you-know" authentication methods actually increases fraud due to tactics such as MITM attacks.

Criminals are using automated attacks through online and mobile channels to exponentially expand the account-takeover fraud damage. Both financial and secondary accounts, such as email accounts, are targeted because they provide criminals with validity and help them conceal the crime, as email accounts are often the destination for password-change alerts.

Moreover, there's a false sense of security as Touch ID and other native phone biometrics don't eliminate password vulnerability. They simply make it easier for consumers to unlock their phones.

Consumers' expectations of convenience, combined with a general lack of knowledge about security, compound the issue. Consumers expect ease of use in their payments and retail and bank accounts, but at the same time, they blame the merchant or bank when an account takeover happens.

HOW ECOMMERCE SMBs ARE FUTUREPROOFING THEIR BUSINESSES IN THE WAKE OF PAYMENTS EVOLUTION

Oscar Nieboer – CMO, Paysafe Group

Security has overtaken reliability and cost as the top priority for businesses when selecting a PSP. Here's why.

There is a genuine belief globally that online goliaths such as Amazon, with the financial and human resources at their disposal to be at the cutting edge of all and any industry it chooses, have their eyes fixed on running every small competitor out of business; the online businesses that cannot keep pace with the latest innovations in customer experience will fall away as their market consolidates.

To discover how businesses are reacting to this threat, we asked over 600 SMBs from across Europe and North America accepting payments online to tell us how they are planning to future-proof their businesses in the face of a rapidly changing ecosystem and with eCommerce power-houses looming over their shoulders.

CHOICE IS FUNDAMENTAL AT THE CHECKOUT OF TOMORROW

One major takeaway from our *Lost in Transaction: The future of payments for SMBs* research is that online businesses are committed to giving consumers more flexibility when it comes to the method for making a payment.

According to our survey, 75% of online businesses agree that increasing the number of payment methods they offer at the checkout is essential to success. This is a recognition that the payments ecosystem is fragmenting, with consumer payment preferences dissipating beyond traditional card payments to numerous alternative payment solutions.

Online businesses currently offer four payment methods on average, but this is predicted to rise to six within two years. The alternative payment

methods we expect to feature more regularly at the checkout after this time include online cash replacement systems, payments by instalment, and subscription payments.

IN THE ERA OF SEAMLESS PAYMENTS, SECURITY TRUMPS EVERYTHING ELSE

Online businesses are aware of the pressure to create a seamless payments experience, but over half (52%) of them also believe that reducing friction in the payments process exposes them to a greater risk of facilitating fraud. 74% believe fraudsters are targeting online businesses more than they were this time last year in any case, and 55% acknowledge that online card fraud is an increasing problem for them.

So it's not surprising that security is now the primary factor online SMBs take into consider when selecting which payment service providers (PSPs) to partner with. 59% of businesses list security as a key consideration, ahead of reliability (49%) and cost (47%).

This is a direct response to the need to implement friction free payments in a secure way to remain competitive; 81% of businesses place the responsibility for protecting against fraud at the door of their PSP and 70% acknowledge they are finding it hard to determine the balance between improving security processes whilst making the customer journey as seamless as possible. Overcoming this hurdle is the critical step to futureproofing for an online merchant, which is why it is such a critical consideration factor when selecting a payments partner.

In today's consumer-driven environment, convenience is considered table stakes for a good customer experience. Nearly 40% of consumers would change their banks for a better mobile app. This new lack of stickiness underscores the importance of driving convenience at every stage of the customer's journey.

While companies are hesitant to disrupt consumer convenience, ATO can severely damage brand reputation among customers. When debating between the two, consider the lifetime value of a lost customer.

The key to thwarting ATO attacks is detection at login. And while many merchants worry about increasing consumer friction through added security, there are many fraud-prevention tools designed to be transparent and consumer-friendly.

Everyone's Business

Only about half of consumers are familiar with online/mobile authentication, and this number is likely lower for certain segments of the population, like Baby Boomers.

Because Millennials are more likely to be acceptors and early adopters of security measures, it is important to focus on giving them the education and tools to continue fostering their openness towards fraud prevention and security.

But while a lot of businesses are focusing on Millennial engagement, it's also imperative to focus on educating the generations that are not as accepting of this new technology. Take a good look at the ways you educate your entire customer base about security solutions, especially older generations who lack awareness or understanding of identity theft and other security threats.

It's important to communicate the damage account takeovers can do. By doing this, you can educate your entire customer base on the more secure encryption offerings available to prevent identity theft.

Consumers know that passwords, by themselves, are not the best security method. Yet, there are many misconceptions about which security solutions work. Customer knowledge and participation is key to driving stronger, practical security options at account opening and beyond.

No Silver Bullet

When it comes to eliminating digital fraud, there's no one-size-fits-all approach. However, accuracy and response times are critical in reducing it.

Financial institutions need to explore the online-account and fraud-detection solutions that work best for them, including ones that offer more insights into consumers' identities and provide the ability to stop fraud at the login process. This is a key way to prevent enterprisewide and multi-channel ATO.

There are also many protection services that combat ATO at login. Monitoring geographic IP change, device change, password-entry behavior, time-of-day differences, and browsing time before logins can be impactful in thwarting ATO, without harming the consumer experience.

Account takeover numbers are increasing exponentially, with some reports indicating year-over-year growth as high as 160%. This high number, combined with the higher number of solutions to tackle this issue, can be overwhelming to merchants and financial institutions.

While there is not one solution that reduces this number to zero, the goal is to see numbers trending down. Financial institutions and card issuers can take certain steps to improve security in their digital channels without adding friction to the customer experience.

With the proper technology and monitoring solutions, you can help significantly reduce ATO at login and protect your customers' most important data, without causing them to completely disengage from your brand. **DT**

Enjoying the view?
Wait until you see your portfolio.

Partner with
HUMBOLDT

At Humboldt Merchant Services, helping you grow your portfolio comes naturally to us. After all, we've been providing customized payment acceptance solutions to retail, ecommerce, and specialty merchants since 1992. So partner with Humboldt today and take your profitability sky-high with solutions for every merchant, **all supported by**:

Specialized Chargeback Reporting.

Multi-Currency Conversion.

A Full Suite of Anti-Fraud Services.

A Boutique Client Experience.

Whole new revenue streams for you, plus the unparalleled personal service you and your merchants deserve ... How's that for a breath of fresh air?

JOIN THE 25-YEAR INDUSTRY LEADER TODAY.
855.767.0685 | HBMS.COM

INDUSTRIES WE SPECIALIZE IN:
Adult Content · Bail Bond Insurers · Business Opportunity · Buying Clubs · CNP Tobacco · Dating
Direct Marketing · E-Cigarettes · Extended Warranty · Firearms & Ammunition · And Many More