

DIGITAL TRANSACTIONS

Trends in the Electronic Exchange of Value

WHATEVER HAPPENED TO ENCRYPTION?

Equifax wasn't alone in neglecting this data-masking technology. Here's what's happening to change that.



ALSO IN THIS ISSUE

- Visa's Lonely Vigil for Signatures
- A Niche Play in Bitcoin Acquiring
- Why P2P Is Coming to the Cash Register
- Will Checkout Always Be a Hassle?

One Provider. Multiple Options.

ProPay® — making payments and payouts easy for marketplaces and platforms.

ProPay, a TSYS® company, is a single source provider with multiple ways to process payments securely, and disburse funds affordably and efficiently.



Payment Processing:

Global payment processing (credit cards, ACH)



Payouts for Platforms:

Pay commissions globally in over 130 currencies



Fraud Protection:

Prevent against theft with Guardian CyberShieldSM



Payment Security:

Encryption and tokenization service with ProtectPay[®]



Automatic card updating:

Reduce card declines with EnsureBillSM

Trust ProPay. We provide unique payment solutions to payment facilitators, platforms and marketplaces.

For more information, call **888.227.9856**, email **sales@propay.com** or visit **www.propay.com**

All trademarks contained herein are the sole and exclusive property of their respective owners. Any such use of those marks without the express written permission of their owner is prohibited. ©2017 ProPay Inc. All Rights Reserved. TSYS® is a federally registered service mark of Total Systems Services, Inc. All rights reserved. TS7617

PROPAY
A TSYS® Company



Accelerate your career with Harbortouch

The most successful **POS**
program in the payments industry

- ☑ Best-in-class Elite POS & Tablet-Killer Echo POS
- ☑ Solutions for Bar & Restaurant, Retail, Salon & Spa, Delivery
- ☑ POS delivers a more stable and profitable portfolio

Free Leads

Receive warm leads every month from our digital marketing and telesales initiatives

Reward Point Program

Earn points for every deal that can be redeemed for exciting prizes

\$25,000

Signing Bonus

12x/\$400

Terminal Bonuses

up to \$5000

Free VX 520 Terminals

VIP Program

Obtain higher quality merchants with special incentives and VIP support

\$100+ billion processed annually | **1+ billion** transactions annually

Now offering PCI-validated P2PE, tokenization, EMV and offline EMV processing

For more information, contact:

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

or visit www.isoprogram.com



HARBORTOUCH
A LIGHTHOUSE NETWORK COMPANY

CONTENTS

January 2018 ■ Volume 15, Number 1

26 Whatever Happened to Encryption?

Widely touted as a potent data-masking tool, encryption has been slow to take hold in the payments industry, despite a continuing plague of data breaches. Here's what's going on to change that.

4 The Gimlet Eye

Serving the Small Merchant

6 Trends & Tactics

As Its Rivals Write off Signatures, Visa Stands Alone

With Discover and AmEx joining Mastercard in ditching signature authentication, guess who remains silent on the issue?

How E-Commerce Is Changing Point-of-Sale Payments

The explosive growth of e-commerce may be shutting down some stores, but its effects on the point of sale are even more far-reaching than that.

The End of the Line for Chicago's Open-Loop Transit Cards

Why the CTA couldn't make a go of its network-branded Ventra card.

The Inside-Out EMV Conversion at Gas Stations

The forecourt can come later. Right now, petroleum marketers are focusing on the c-store.

Did Banks Blow It by Spinning Off Visa and Mastercard?

AmEx's Ken Chenault sets off a debate over the philosophical underpinnings of a payment network.

Plus, Security Notes warns that too few security pros consider the "day after," and Payments 3.0 says faster payments may be here before you know it.

'Data security is a game of leapfrog. Build a 10-foot wall and the hackers will come back with a 12-foot ladder. EMV still sends card data in the clear.'

PAGE 26

16 Acquiring

Bitcoin Accepted Here?

For all the hype lately, the digital currency remains a niche opportunity for independent sales organizations and other third-party acquirers.

20 M-Commerce

P2P And Beyond

Suddenly, person-to-person payments services are gaining utility beyond just paying a person via a smart phone. What gives?

34 E-Commerce

Are We There Yet?

What's happened to the e-commerce checkout and why it isn't easier to make a payment.

38 Endpoint

Why PIN on Glass Is the Next Big Thing

The key to higher acceptance rates for cards, lower fees for merchants, and better security for all lies in moving the point of sale from hardware to software, says Sam Shawki.

Cover illustration: Jason Smith, Fotolia.com

MagTek's New Year's Resolution

Deliver secure, reliable, and flexible payment hardware and services.



kDynamo

Break free from the checkout line in 2018 with this flexible device. Accept magstripe, EMV chip cards, and NFC payment transactions.



Security

Safeguarding consumers and their personal information with payment solutions that protect anytime and anywhere.



eDynamo

Go mobile this year with our secure card reader conveniently accepting both EMV chip cards and magstripe cards.



FIND OUT MORE ▶

☎ 562.546.6467
✉ sales@magtek.com
🌐 www.magtek.com



Serving the Small Merchant

Seldom in the history of electronic payments has the spotlight shone quite so intensely on small merchants as it does now. Everybody, it seems, wants to sign up the so-called SMB—the small and medium-size business.

When Total System Services Inc. (TSYS) put up just over \$1 billion last month to buy Cayan, a large part of the rationale was to pick up Cayan's portfolio of 70,000 SMBs. And Cayan is just one, though also one of the more successful, of the processors and gateways catering to small merchants with sophisticated point-of-sale technology that allows the businesses to accept EMV cards and digital wallets while at the same time melding together data flows from both stores and the Web.

With TSYS's resources behind it, Cayan may be able to expand the reach of this technology to more SMBs. That's a trend that will dovetail nicely with a parallel movement among software developers to focus on helping small companies integrate payments with their accounting and POS systems. That movement has been in progress for several years, but is picking up steam lately as developers recognize the opportunity in helping merchants figure out how to scoop up and make sense of payments data.

At the same time, the industry has witnessed over the past few years the rise of the so-called payment facilitator. This entity, which may be an independent sales organization, an independent software vendor, or just a larger merchant, eases the entry of small merchants into the payments network. The small merchant simply rides on the merchant account of the ISO, ISV, or online marketplace, dispensing with the need to apply for its own account and saving considerable time and money.

This device has made it possible for tens of thousands of very small businesses, even flea-market sellers and other occasional merchants, to gain access to the same electronic-payments systems that Walmart uses.

To be sure, none of this is perfect. One reason small businesses are attractive to processors is that they lack negotiating heft, and so generally end up paying higher rates than their larger cousins. As for technology, not all merchants need the slickest loyalty integration on offer. And the payment-facilitator model may prove a bit too facile for some, leaving them exposed to risk they hadn't counted on.

But the general drift—toward better service, better access, better technology, faster set-up—is a significant improvement for the small merchant over what was available only a few years ago. It's also a good deal for the acquiring industry, opening up, really for the first time, a vast market that, in the aggregate, accounts for a dynamic slice of the U.S. economy.

John Stewart, Editor | john@digitaltransactions.net

PUBLISHER

Robert A. Jenisch

EDITOR-IN-CHIEF

John Stewart

Senior Editor

Jim Daly

Senior Editor, Digital

Kevin Woodward

Correspondents

Jane Adler

Lauri Giesen

Karen Epper Hoffman

Peter Lucas

Linda Punch

Elizabeth Whalen

Art Director/Production Editor

Jason Smith

Editorial Advisory Board

Eula L. Adams

John Elliott

Alex W. "Pete" Hart

Former Chief Executive Officer,

MasterCard International

William F. Keenan

President, De Novo Corp.

Dr. Gideon Samid

Chief Technology Officer,

AGS Encryptions Ltd.

Director of Advertising

Robert A. Jenisch, 877-658-0418

bob@digitaltransactions.net

Advertising Sales Representatives

Robert Mitchell, 877-658-0418

bmitchell@digitaltransactions.net

Cathy Woods, 602-863-2212

cathy.woods@mediawestintl.com

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

John Stewart, Managing Director

Robert A. Jenisch, Managing Director

For advertising information, call 877-658-0418.

To subscribe or give us a change of address,

go to www.digitaltransactions.net and click on

"Subscriber Care" or call 847-559-7599.

The views expressed in this publication are not necessarily those of the editors or of the members of the Editorial Advisory Board. The publisher makes reasonable efforts to ensure the timeliness and accuracy of its content, but is not engaged in any way in offering professional services related to financial, legal, accounting, tax, or other matters. Readers should seek professional counsel regarding such matters. All content herein is copyright © 2018 Boland Hill Media LLC. No part may be reproduced without the express written permission of the publisher. Subscription prices: \$59/year for subscribers in the United States; \$69/year for Canadian subscribers.

All other subscribers, \$119/year, payable in U.S. currency.





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.



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

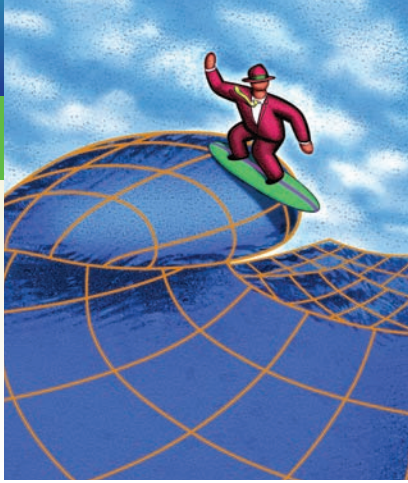


US Headquarters:

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



TRENDS & TACTICS

As Its Rivals Write off Signatures, Visa Stands Alone

Three of the four U.S. general-purpose card networks—American Express Co., Discover Financial Services, and Mastercard Inc.—now plan to cease requiring signatures for point-of-sale transactions made with their cards beginning in April. That leaves Visa Inc. as the sole signature supporter.

AmEx on Dec. 11 joined Mastercard, which started the no-signature movement in October (“Signing Off,” December, 2017), and Discover, which changed its policy a few days before AmEx. Discover said its signature requirement would end for transactions in the U.S., Canada, Mexico, and the Caribbean. AmEx’s change applies worldwide, though the company says cardholders may still sign if a merchant asks or local law requires a signature.

AmEx says the need for signatures has declined because of improving anti-fraud measures and other changes in payments, including the introduction of EMV chip cards, the growth of contactless payment options, and the continued expansion of online commerce.

Plus, AmEx wanted to make shopping with its cards similar everywhere.

“American Express decided to make this change globally because it

will enable a more consistent check-out experience across all regions,” an AmEx spokesman says in an email. “A key example of this would be situations when a U.S. cardmember travels outside of the U.S. to a country that is primarily chip-and-PIN and makes a purchase at a merchant with their U.S.-issued card. Currently, that merchant may require the cardmember to sign their receipt because our U.S. consumer cards are not enabled with PIN.

“As a result of our policy change, in April 2018, that merchant could

choose not to collect the cardmember’s signature, which may speed up the checkout process and make the experience more consistent with how other local cardmembers check out.”

The issue of requiring signatures in the U.S. intensified with the advent of EMV chip cards in 2015. Merchants contend that a PIN represents a better authentication method, but issuers and the card brands have been reluctant to add them to credit card transactions because of the possible disruptive aspect of educating

‘With Mastercard and AmEx giving up on signatures, it seems inevitable that Visa will follow.’

—Thad Peterson, senior analyst, Aite Group LLC



BITCOIN. THE FUTURE.

Aliant Means **Innovation** in
Merchant Solutions. Get Started.



ALIA NT

+ BITCOIN PROCESSING + HIGH RISK PROCESSING + PAYMENT GATEWAY

+ ECOMMERCE INTEGRATION + INDIVIDUAL HANDS-ON SUPPORT

Get Started Today | 888.638.6103 | aliantpayments.com

consumers. Now three of the four card brands have leapfrogged over that.

After AmEx's announcement, Visa said it supports multiple technologies "to bring speed, security, and consumer convenience to the authentication and authorization process." That was the same statement it issued in October.

But industry observers speculate Visa will follow the other brands.

"With Mastercard and AmEx giving up on signatures, it seems inevitable that Visa will follow," says researcher Thad Peterson, senior analyst with Boston-based Aite Group LLC.

Merchant groups express similar views.

"I can't imagine how Visa could respond to investor, customer, and

other public inquiries as to why they believe signature is a valid and worthwhile CVM [cardholder verification method] when every one of their competitors' actions indicate otherwise," says Laura Townsend, senior vice president of operations at the Minneapolis-based Merchant Advisory Group.

—Kevin Woodward

How E-Commerce Is Changing Point-of-Sale Payments

And speaking of what goes on at the point of sale, the seemingly unending growth in online shopping is doing more than closing physical stores. The point of sale in the stores that remain is changing, and along with it, payments providers, according to Javelin Strategy & Research.

As consumers continue to increase their spending online rather than in stores, retailers and their payments providers will have to adapt more than they have already, says Michael Moeser, director of payments at Pleasanton, Calif.-based Javelin.

Chief among the findings in Javelin's recent "2017-2021 Retail Point of Sale Payment Forecast" report is that the sales shift from physical stores to online ones will come at the expense of face-to-face transactions. U.S. e-commerce sales will grow 37% from \$518 billion in 2016 to \$708 billion by 2021, while retail sales in physical stores will slip 1% from \$4.4 trillion to \$4.36 trillion (chart).

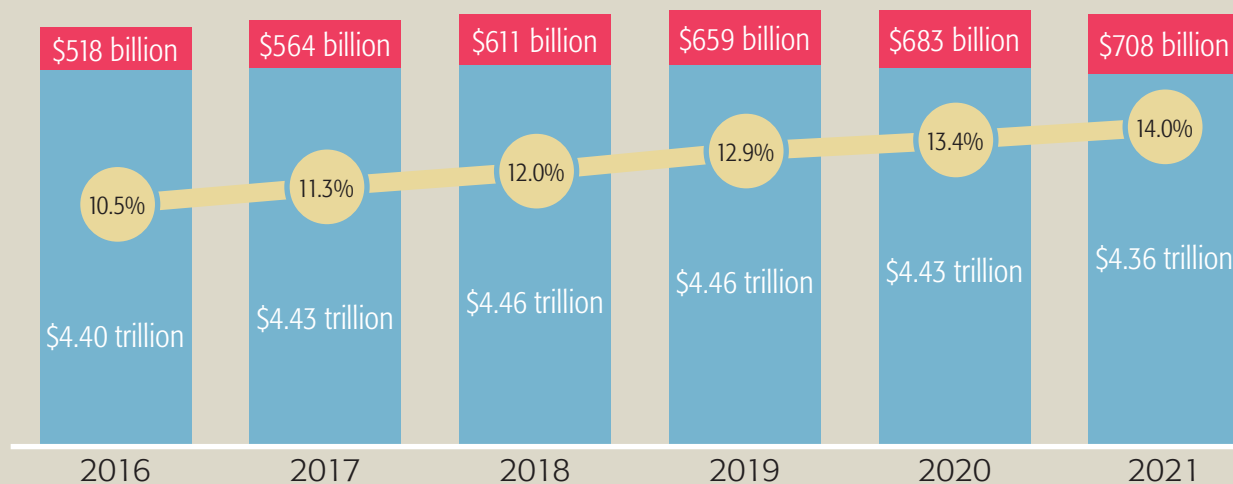
Javelin estimates e-commerce accounted for 11.3% of total U.S. retail sales in 2017, up from 10.5% in 2016 and 8.9% in 2015.

For payments companies, online retail growth does not signal a diminution of the importance of POS sales, Moeser says in an email to *Digital Transactions*.

"The important thing to remember is that many physical merchants also have a digital presence, however, many times there is a lack of coordination between the two," Moeser says. "Oftentimes, the Web site by a storefront merchant has a different acquirer, which can make it difficult when a consumer buys something online and brings it into a store for a

The Forecast for Unabated E-Commerce Growth

■ U.S. Retail POS Purchase Volume ■ U.S. E-Commerce Purchase Volume ● E-Commerce as % of Total Retail Sales



Source: Javelin Strategy & Research

return or exchange. Having the same acquirer can often help solve the payment side of this transaction.”

Merchant acquirers will want to sell card acceptance for both in-store and digital systems, despite the often different sizes of the two businesses, he says.

“For example, a storefront may run 80% of the revenue and the Web site only 20%. So to have two different acquirers doesn’t make sense for the store or either acquirer. In this case, it behooves an acquirer to sell both services.”

The report cites other changes, such as a decline in paying with paper checks, growth opportunities for credit and debit cards, and a potential expansion of mobile payments and wallets.

Moeser predicts that mobile-wallet use, in particular, will “explode starting in 2018.” A big reason for that is that merchant-based mobile wallets, such as Walmart Pay, Kohl’s Pay, and Target Wallet have something that multiretailer wallets have yet to achieve: retailer engagement.

“The value of a Walmart, CVS, or Target-type retailer wallet is that it holds a rewards card or program so you no longer need to carry a physical card or something on your key chain, coupons, receipts, payment cards, prescriptions or other standing orders, and more,” Moeser says. “Yes, having a CVS wallet is not going to help you at Target or Walmart, but it will help you if CVS is a place where you spend 25% to 50% of your retail dollars or it’s somewhere you go to get a prescription.”

Consumers will have only one or two retailer wallets for places they shop frequently or have important things they need to keep track of such as a prescription, he adds.

—Kevin Woodward

The End of the Line for Chicago’s Open-Loop Transit Cards

The Chicago Transit Authority, an early proponent of open-loop fare payments, is getting out of the business of offering fare cards that doubled as a Mastercard prepaid card, giving pause to advocates of combining transit fare media with general-purpose payment cards.

The CTA announced early last month that the general-purpose payment feature in some of its fare cards would expire Dec. 31. The operator of the nation’s second-largest transit system says riders did not embrace the offering.

The CTA’s fare-payment system, dubbed Ventra, is managed by Cubic Transportation Systems and includes First Data Corp. as a subcontractor. Among the fare options that became available when Ventra launched in 2013 under a 12-year, \$454 million contract was a contactless Mastercard-branded prepaid card good at any

Mastercard-accepting merchant as well as on CTA buses and “L” trains.

“After analyzing customer preferences and habits, CTA determined that there wasn’t significant demand for this feature,” the agency said in a press release.

The CTA attributed that lack of demand in part to “the numerous prepaid debit products in the marketplace and electronic payment options like Apple Pay, Android Pay, and Samsung Pay, which have become more accessible and provide consumers with increased financial options, including the ability to pay their Ventra fares.”

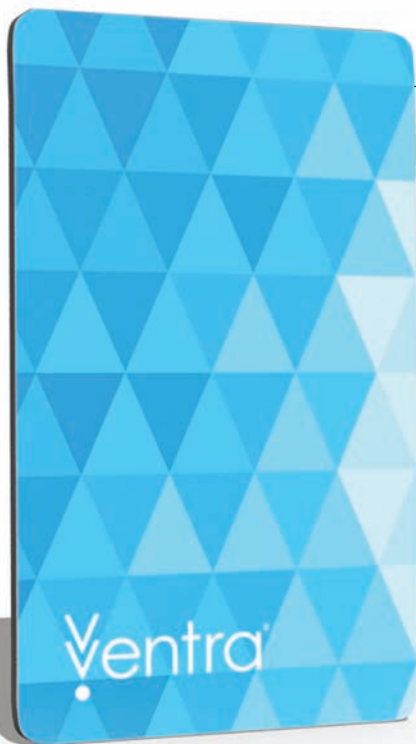
New, closed-loop Ventra cards went on sale in mid-December. Customers who had Ventra Mastercard cards could have their balances transferred to prepaid cards offered by First Data’s Money Network, which provides cards issued by Meta Financial Group Inc.’s

USAPAY 20 YEARS

ALWAYS AHEAD OF THE GAME

866.490.0042 USAePay.com USAePay/ [Facebook] [Twitter] [LinkedIn]

The advertisement features two fishbowls on a dark surface against a blue background. The left fishbowl contains a splash of water with a small rocket ship (USAPay logo) emerging from it. The right fishbowl contains several goldfish. The text 'USAPAY 20 YEARS' is in the top right, 'ALWAYS AHEAD OF THE GAME' is in a blue box in the middle right, and contact information is at the bottom.



(Image: Chicago Transit Authority)

The CTA's updated closed-loop Ventra card.

MetaBank. Or, they could spend down their balances by the end of the month or have their funds returned via check from Money Network.

A CTA spokesperson did not respond to a *Digital Transactions* email requesting further comment.

The CTA will continue to accept open-loop media for fare payments issued by other entities that support contactless transactions, according to transportation payments consultant Peter Quadagno of West Chester, Pa.-based Quadagno & Associates Inc. Besides mobile wallets, they include general-purpose payment cards with EMV chips that also are equipped with near-field communication (NFC) antennas to enable contactless payments. There are few such “dual-interface” cards currently available in the U.S., however.

Although an increasing number of transit agencies are accepting open-loop contactless payments, especially through mobile wallets, few yet have

jumped into general-purpose issuance, although more might try.

The CTA was the only major system in the U.S. issuing such media, though the Southeastern Pennsylvania Transportation Authority (SEPTA) in Philadelphia is planning to offer a Mastercard-branded SEPTA Key card among its fare options under a new payment system. Transit agencies in New York City and Boston also are mulling general-purpose card issuance under new contracts with Cubic, Quadagno says.

But general-purpose prepaid fare cards, which involve working with program managers and other entities, can be more expensive to provide than closed-loop fare media, according to Quadagno.

“They [agencies] have realized that the economics don’t work in the U.S., and so they’re backpedaling,” he says. “The lesson is, make sure you understand the business rationale before you go off and do it.”

—Jim Daly

The Inside-Out EMV Conversion at Gas Stations

U.S. gasoline retailers are finishing up their EMV chip card conversions inside the convenience store before they turn their full attention to fuel pumps, industry executives say. But as the conversion gathers steam, fuel retailers are facing a shortage of technicians qualified to do the work.

C-stores and standalone gas stations caught a break a year ago when Visa Inc. and Mastercard Inc. postponed their planned October 2017 EMV liability shifts for unattended fuel dispensers for three years. Almost no fuel retailer would have been ready by then, and going into 2018 the pump conversion is still moving slowly.

When asked in December what percentage of U.S. automated fuel

dispensers are ready to accept chip cards, one industry expert who requested anonymity pegged the number as “very low.”

That’s not surprising, considering that only six months earlier Gilbarco Vedder-Root, a big fuel-pump manufacturer, announced what it claimed to be the first EMV transaction coming from a U.S. pump. That leaves somewhere north of 1 million more dispensers to go.

“There is no chain out there that is rolled out, big or small, that is EMV-operational on the dispensers,” says Gray Taylor, executive director of Conexus Inc., an Alexandria, Va., a standards and technology non-profit that was spun off from NACS, the national convenience-store trade group.

What’s happening, he says, is that c-stores and gas stations are converting to EMV from inside the store first, and then out to the forecourt where the pumps are located. More so than with most merchants, electronic payments at gasoline retailers must be integrated into complex networks that include pumps on the outside, and point-of-sale terminals, controllers, wired or wireless systems, and related technology inside.

“That is a predecessor to getting outdoor ready,” says Terry Mahoney, a partner at Chicago-based W. Capra Consulting, which works with petroleum retailers and industry vendors.

Many operators still aren’t done with their stores, but work generally is



(Photo: Wayne Fueling Systems)

The scarcity of EMV-certified fuel pump technicians 'is the most significant bottleneck out there.'

—Tim Weston, technology solutions sales manager, Wayne Fueling Systems LLC

Wayne Fueling Systems' iX Pay EMV-accepting platform for gasoline pumps.

progressing well, especially at larger gasoline retailers, according to Taylor. "The inside—we're feeling pretty comfortable," he says.

Mahoney predicts that some time in 2018 the majority of transactions inside c-stores will be chip-on-chip: a functioning EMV POS terminal reading an EMV credit or debit card.

Meanwhile, payment card-accepting hardware and software providers that supply petroleum retailers, including San Jose, Calif.-based VeriFone Systems Inc., have complained that the liability-shift postponements have delayed expected revenues because they supposedly gave a reason to gas stations to put off their EMV upgrades.

Tim Weston, technology solutions sales manager at Austin, Texas-based pump manufacturer Wayne Fueling Systems LLC, agrees that has happened with smaller, independent c-store operators.

"As a group, they're the folks that have taken their foot off the gas, so to speak," says Weston, adding that some small operators hope the major oil companies will come up with subsidies to offset part of their conversion costs. Their hopes have yet to be realized.

Upgrade expenses are considerable. An EMV retrofit kit for one pump handling two opposite-facing dispensers can cost \$5,000 or more. W. Capra Consulting has estimated total U.S. conversion costs at up to \$6 billion.

Beyond costs, a major emerging issue is the scarcity of technicians certified to do the EMV upgrade work. One c-store executive recently pegged the number at only about 3,000 in all of the United States. These technicians must visit approximately 150,000 gas stations, many with 16 pumps.

"That's the most significant bottleneck out there," says Weston. "That population of trained and certified technicians is a limited population."

Taylor is of like mind regarding pumps getting certified as meeting EMV requirements. "We're probably where everybody wanted to be two years ago," he says. "It is a big bottleneck."

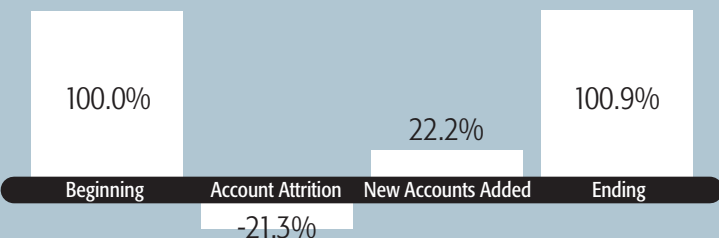
—Jim Daly

MONTHLY MERCHANT METRIC

Q3 2017 Account Attrition And Growth

Account Attrition—Total attrited accounts in given period divided by total portfolio active accounts from same period of the prior year.

New Accounts Added—Total new accounts in given period divided by total portfolio accounts from same period of the prior year.



Note: This is sourced from The Strawhecker Group's merchant data warehouse of over three 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.

Source: The Strawhecker Group © Copyright 2017. The Strawhecker Group. All Rights Reserved. All information as available.



Did Banks Blow It by Spinning Off Visa and Mastercard?

Outgoing American Express Co. chairman and chief executive Ken Chenault may well have touched off a debate about what constitutes the ideal governance structure for a global payments network.

Chenault, who will retire next month, charged in December that the former owners of his two leading rivals, Visa Inc. and Mastercard Inc., committed a big mistake when they spun off to the public what had been bank card associations. In response, critics counter that AmEx's own management model has fallen short in recent decades.

Speaking at an investors' conference in New York City, Chenault called the decision to have Visa and Mastercard go public "one of the biggest strategic blunders of the last 20 years," according to an account of his talk reported by Bloomberg.

Mastercard's initial public offering took place in 2006, while Visa's came two years later. The moves followed decades of ownership of both companies by financial institutions, which operated the networks as not-for-profits.

In large part, the spinoffs were a hedge against the risk posed by antitrust lawsuits merchants had filed starting in 2005 that challenged the networks' interchange-pricing practices. Those suits, now consolidated, will be heard in federal court in Brooklyn, N.Y., following the collapse of a \$5.7 billion settlement last year.

Chenault argued the IPOs badly undervalued the two companies and cost the banks crucial control over payments economics and developments.

"They didn't understand what they were giving up, and they lost sight of where the puck was going,"

Chenault said at the conference, according to Bloomberg. "Along with yielding pricing power to the network, the banks also limited their access to data and merchant relationships at a critical time."

Visa's IPO, the biggest in U.S. history at the time, was priced in the midst of a bear market at \$44 per share for 406 million shares. Mastercard's offering sold 66 million shares at \$39 each. Visa's share price closed Dec. 15 at \$113.82, and Mastercard's at \$153.40.

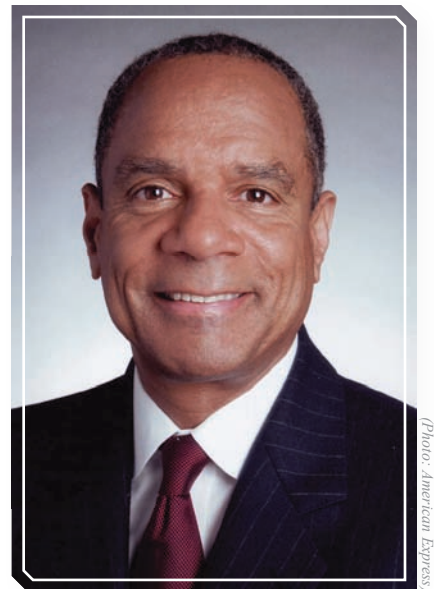
The transfer of both wealth and control, Chenault added, was "unbelievable." As a result, financial institutions are now reduced to serving the networks' interests rather than the other way around, he charged.

This picture, he said, contrasts with the situation at AmEx, which has been able to steadily introduce services to win customers. "We can't be reduced to simply facilitating a payment," he said.

A Mastercard spokesperson would not comment on Chenault's remarks. Visa did not respond to requests for comment.

What Chenault forgets, critics say, is that public ownership has over time yielded far better results for Visa and Mastercard than AmEx's model has done for AmEx.

"It's worth recalling [that] in the [United States] in the 1980s American Express, Mastercard, and Visa in payment volume were roughly the same size. Today, in the only national market where the AmEx network is material—the U.S.—it has [approximately] 10% of payment volume," notes Eric Grover, principal of Intrepid Ventures, a payments consultancy based in Minden, Nev. "The open-network model has proved stronger than the



(Photo: American Express)

Banks "didn't understand what they were giving up" by spinning off Visa and Mastercard, contends AmEx's Chenault.

closed-loop model in building network scale in the U.S. and globally."

Moreover, the spinoffs increased the networks' underlying value for financial institutions, consumers, and other payments players, contends Grover, a former Visa executive.

"When thousands of banks collectively owned Mastercard and Visa, they were run as not-for-profit bank card utilities. The assets underperformed," he says. "Their IPOs unshackled Mastercard and Visa from association governance and, as independent payment networks, they became more enterprising and aggressive."

On one key point, however, Grover agrees with Chenault. In Mastercard's case, at least, the offering was undervalued, he says.

"Partly, that was because in 2006 there were no obvious network-valuation comparables," Grover says. "Many analysts used public payment processors as valuation benchmarks. The market didn't appreciate the enormous power of a retail payment network with global critical mass." **DT**

—John Stewart

The Database Battleground



Gideon Samid • *Gideon@BitMint.com*

Cyber fraud has matured into a solid industry, where economies and efficiencies count. So the lion's share of hacking efforts is directed at large databases, where a breach is a gift that keeps on giving (as long as it is well-managed). Finan-

cial institutions and online merchants, in particular, use databases that constitute a juicy target for the cyber-fraud industry because of how productive a successful penetration may be.

We on the security side are not strategically prepared for the challenge. We are overly impressed by breaches of individual phones and devices, where the damage is limited and the responsibility lies with the individual user. When it comes to our crown jewels, the financial database, we naturally tend to minimize our vulnerabilities.

Typically, chief information officers are very much taken with the enormous work they invest in installing the latest intrusion-detection software and with the countless coordination meetings they hold, where they design sophisticated security protocols. Their overconfidence leads to fateful decisions against data-at-rest encryption, and against double-checking already-admitted users.

We can rate database vulnerability according to: (i) how attractive its content is; (ii) how many users, and at what levels of credentials, it serves; (iii) how heterogeneous its operations are; and (iv) whether the security team has a good computer-science education. The combination of theoretical flaws (technology and protocols), implementation flaws (bugs and malware), and human factors (stupidity, greed, and indifference) is a reliable predictor of the prospect of compromise.

Complicating matters is that the new hacker tactic is to exploit a breach ever so meagerly to remain undetected, sometimes for years.

To deny this reality with false confidence is not a good strategy. Instead, we need to ask ourselves how to survive a successful penetration. When a database is exposed, the hacker learns private information about the listed customers. Much of this private info will help hackers crack other places where the same data is used. It is therefore a strategic

goal to reduce the hacker's profit from a successful breach.

There are two tactics for doing this. The basic one is replacement. In two previous "Security Notes" columns (June and July 2016), I presented the Cyber Passport concept, which is designed to quickly replace private-access credentials and render the data ineffective.

The second, more ambitious move is to use cryptographic means to fingerprint the credentials database. If the system is breached and that data is compromised, the hackers will not be able to use it to claim access in the name of the original owner of the data. This protection applies also against insiders abusing their access to steal credentials files and peddle them in the dark market.

As this technology takes hold, the payoff for hackers will diminish and they will gradually abandon their strategy to penetrate financial databases. They might turn their efforts to retail theft, attacking one individual victim at a time. Or, one must admit, they might surprise us with a move we are not imaginative enough to foresee.

Other variations on these tactics include sub-encryption: encrypting data with fast, half-transparent ciphers, which impose enough cryptanalytic burden that the effort to crack the data is too taxing relative to the potential benefit. Remember: Now that hacking is no longer a matter of emotional bravado, but a full-fledged industry, it surrenders to the same laws of return on investment that govern the rest of us.

In 1998, Ron Rivest (the "R" of RSA) proposed a "winnowing and chaffing" strategy that mixes the good data with nonsense data such that hackers cannot separate them. His original idea has since been replaced by more effective means, but the principle is still valid and useful.

One side benefit of these new cryptographic tactics is that, for most of them, it is easy to install a breach monitor—a means to detect that a request for credentials is based on compromised data. This detection may lead to stealth-tracking of the source and to preset countermeasures.

The technology is there. What is needed is recognition that the database is the modern cyber-war battlefield, and that the hackers have a non-negligible chance to hack into any database with a sufficient number of credentialed users. Therefore, a strategy for the "day after" has to be devised. ■

Faster Payments: Coming Soon



George Warfel • GWarfel@haddonhillgroup.com

Faster payments in the United States took a major step forward in November with the sending of what many consider the first U.S. faster-payment transaction. A payment was made, in seconds, between U.S. Bank and BNY Mellon using

The Clearing House's Real Time Payments system, a system that meets evaluation criteria used by the Federal Reserve's Faster Payments Task Force.

Faster-payments advocates can get into heated debates over what is truly a faster payment. The debate is about more than bragging rights. At stake could be who will make payments to and receive payments from faster-payments systems around the world.

The administrators and regulators of these systems from Mexico to Switzerland will be deciding whom to link with in the U.S. for payments from their faster-payment schemes to U.S. payees. And which sources of payments inbound from the U.S. to accept as meeting their faster-payment criteria. The fact that a U.S. system meets the Task Force's proposal-rating criteria may well be taken by international faster-payment systems as, effectively, a quasi-stamp of approval.

Worldwide, we see standards being set from as fast as "instantaneous" (Singapore) to up to 10 seconds (SEPA PSD.) But how many of the multiple steps involved in processing a payment need to fall within an agreed time limit? Is a message being sent and received within the time boundaries good enough? How about clearing? Or final settlement?

If the payment is a "debit pull," does the time period start when the debit request was generated or is it from when the paying account sends money to the bank originating the transaction request? Or is it when the resulting credit occurs in the specific receiver's account at the bank? What if the funds have been memo-posted to the account but are not yet available funds? Must clearing take place before the time period lapses? And settlement also? But then what if one of the two financial institutions settles every hour or only at the end of the banking day, even if everything else was accomplished in seconds? Standards differ around the world.

The definitions settled on by the Faster Payments Task Force for evaluating and scoring proposals is that a payment must have successfully passed five stages within the time period:

- ▶ Initiation of the payment
- ▶ Debit of the payer's account
- ▶ Credit of the payee's account
- ▶ Clearing of the transaction
- ▶ Settlement between the banks

If this happens in five seconds, the payment system would be considered to be very effective. Over 15 seconds would be considered not effective.

Several systems can meet some, but not all, the criteria within the time limit. To me, the real problem will not be those systems that take somewhat longer than 15 seconds at times, but those that do so consistently.

Some schemes promise payment in seconds—except whenever one of the banks involved needs more time. Then they can take up to, in some cases, half an hour. I call this the airline model: publishing a timetable showing your flight arrives at noon. Except when it arrives at 12:30.

Another limitation is systems that require that sender and receiver both be members of a private scheme. Or both must use a specific brand of distributed ledger or a particular company's electronic coinage.

A critical issue that could hinder some approaches to U.S. faster payments is simply being able to clear and settle 24 hours a day, times 365 days a year. A payment that arrives at a bank at 2 o'clock on a Sunday afternoon would fail to qualify as a faster payment if it didn't clear or settle until Monday morning.

The good news is there is at least one system that meets the criteria and is available (albeit through third parties for some senders or receivers) and there are other systems that come close. Which means the U.S. has at least one qualified system ready to go, and, with some extra effort to overcome the criteria on which the "almost-there" systems didn't qualify, there could be multiple U.S. options to choose from.

It's been a long time coming, but at least one faster-payments system is ready, and others are a step (though sometimes a big step) from being there. ■

Grow your ISO Business Beyond Payments with Paysafe

Take your ISO business to the next level. Paysafe's global partner solutions program provides the necessary financial incentives and business tools to build revenues and expand your merchant portfolio.



Offer a full range of profitable processing solutions including POS and tablet tools



Increase merchant retention with 24/7 dedicated account management



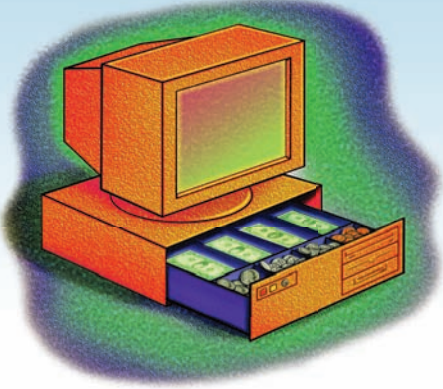
Boost revenues with up-front bonuses, revenue sharing and whole-sale buy rates



Reduce liability and optimize profits with a robust set of risk prevention solutions



Manage your partnerships wherever business takes you with agile online reporting



Bitcoin Accepted Here?

John Stewart

For all the hype lately, the digital currency remains a niche opportunity for independent sales organizations and other third-party acquirers.

On the eve of the 76th anniversary of Pearl Harbor, Valve Corp. dropped a little bomb of its own. The Bellevue, Wash.-based parent of Steam, a marketer of popular online games, issued a statement to say it would no longer accept Bitcoin, effective immediately. The reason? “High fees and volatility in the value of Bitcoin,” the game company said.

High fees? Volatility? That wasn’t supposed to be part of the package with Bitcoin, which promised solid value to merchants when it debuted eight years ago. That value included low acceptance costs, lightning-fast transactions, and, perhaps best of all, no chargebacks. Yes, the price fluctuated, but for the most part within a manageable range.

The result is that roughly 100,000 merchants worldwide accept Bitcoin, businesses ranging from single-unit coffee shops to automobile dealers to big-time online sellers like Overstock.com.

But these days, the experience of sellers like Valve, coupled with head-scratching events in the Bitcoin community, leaves merchants, independent sales organizations, and merchant processors wondering what kind of opportunity lies latent in this newfangled form of money.

“Some people can’t wrap their heads around it,” says Eric Brown, founder and chief executive of Aliant Payment Systems Inc., a 14-year-old, Fort Lauderdale, Fla.-based ISO that’s getting set to offer Bitcoin acceptance to its 7,000 merchants.

Others are taking a more cautious approach. North American Bancard LLC, a Troy, Mich.-based company and one of the biggest ISOs in the country, is considering “a potential pilot in 2018 for a small portion of our [merchant] base,” says Justin Muntean, senior vice president of sales.

But NAB is far from sold on Bitcoin. “We’ve had some inquiries,” Muntean says, “but we haven’t seen a huge surge of interest from our merchant base.”

‘Extreme’ Volatility

Little wonder payments executives and merchants are having a hard time “wrapping their heads” around Bitcoin. It seems there is a negative for every positive these days. Take the cryptocurrency’s most notable feature, its wild runup in value. From roughly \$1,000 at the start of 2017, its price had surged to just shy of \$18,000 by the middle of December.

That has made Bitcoin more notable as an investment vehicle than as a

payment device. Some observers fear it may also encourage users to hold on to the currency, hoping it will appreciate even more, rather than spend it.

Yet that may not be entirely true. BitPay Inc., a major Bitcoin exchange based in Atlanta that processes for 4,400 merchants, has found that people spend more when the price rises because they feel richer, according to a spokesman. And, he says, “the product still has inherent advantages regardless what the price is.”

The numbers may prove him out. BitPay’s merchant volume in 2017 exceeded \$1 billion, up 300% over the previous year. Still, the company is hedging its bets. It plans to add five more cryptocurrencies this year, some as early as this month or February. It won’t say which ones. One popular site, Cryptomarketcap.com, tracks more than 1,300.

Another negative for Bitcoin stems from yet another positive. The currency has become popular enough that its blockchain, the distributed ledger that tracks its transactions across a global network of computers, is struggling to keep up with the traffic. That results in the two big problems that plagued Valve, the game seller: slower transfers and higher fees.

Bitcoin network fees are paid by Bitcoin users when they spend the currency. Early in 2016, when Valve added Bitcoin as a payment option, the fee to its customers was around

Let **ePN** Be Your **EMV Expert!**

Your EMV Eco-System Made Affordable!

eProcessing Network has the secure payment solutions to help you stay current with the technologies that keep your merchants connected. And with real-time EMV capabilities, retailers can not only process contact and contactless payments, Apple Pay and Android Pay, they're able to manage their inventory as well as balance their books via QuickBooks Online.



ePN is EMV-Certified



eProcessingNetwork
the **everywhere** Processing Network™

eProcessingNetwork.com 1(800) 296-4810

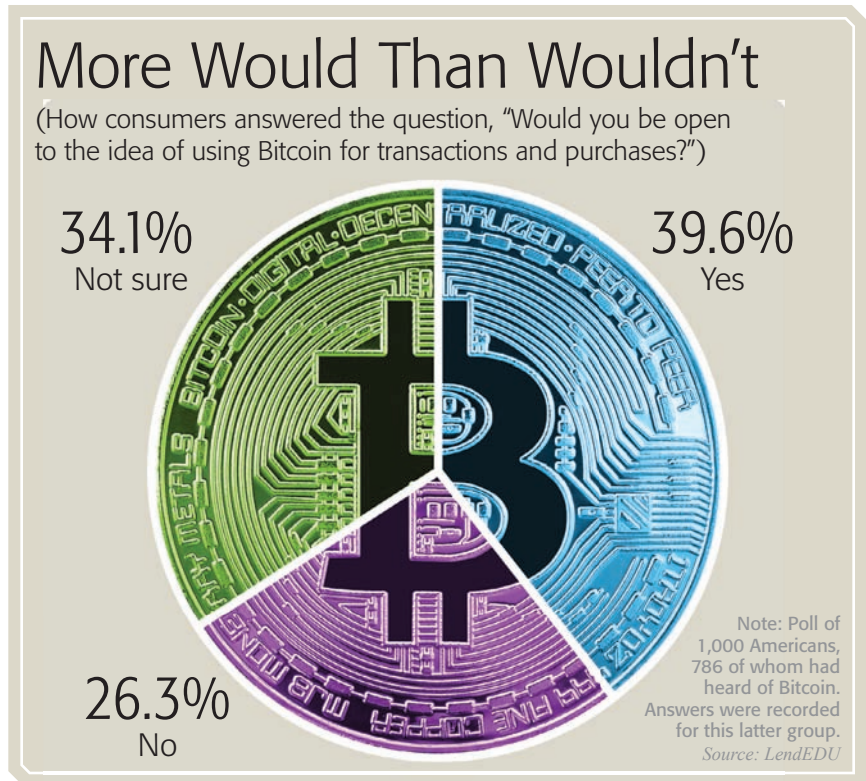
20 cents. By December, it was getting close to \$20.

That was bad enough. What made matters worse, Valve said, is that network congestion had slowed down settlement so much that any downward swing in Bitcoin's value made it necessary to charge the customer again to make up the difference. And that second transaction, of course, triggered a second fee.

While Bitcoin's price has generally surged upward in recent months, that climb has occurred on the back of a jagged arrow featuring some dramatic dips. "Historically, the value of Bitcoin has been volatile, but the degree of volatility has become extreme in the last few months, losing as much as 25% in value over a period of days," Valve noted in its December statement.

Keeping the Lights on

Bitcoin network fees are charged by organizations that harness roomfuls of computers to crack complex mathematical problems. Since the solutions



yield new Bitcoin, these organizations are called miners.

With the buildup in volume, miners have been able to charge more to give transactions priority on the blockchain. That supply-and-demand dynamic isn't likely to change until the developers who manage the network figure out how to boost capacity. One solution, which involves increasing block size, hasn't proved popular enough to be enacted.

Another project, by a group of developers calling themselves the Lightning Network, would take transactions entirely off-chain until the last stage of settlement. That undertaking is nearing the finish line (box, page 19).

But not fast enough for some. Qondado LLC., a 2-year-old developer of encryption software in San Juan, Puerto Rico, last month launched Digital Debit, a mobile wallet that lets users pay merchants—or each other—with Bitcoin. The twist: It gets around network congestion with its own blockchain bypass.

"What we've done is make that experience available right now," says chief executive Edward Robles.

Developed within an application developer network run by San Francisco-based Coinbase, another big U.S. Bitcoin exchange, the Digital Debit wallet interacts with the point of sale by scanning a quick-response code displayed at the merchant terminal.

Once the connection is confirmed, the user can send the required sum through the app, which instantly translates the dollar amount of the sale into Bitcoin. Users must have a Coinbase account, but signing up for Digital Debit automatically creates one, Robles says.

The cost to the user is nothing for transactions under \$10. Over that, it's 50 cents. Qondado keeps the cost down by keeping transactions off the blockchain until the merchant cashes in the newly received Bitcoin, says Robles. "We saw this as a way to be the Apple Pay or Alipay of cryptocurrency," he adds.

But that doesn't mean the system hasn't imposed considerable



(Image: Qondado)

Digital Debit at work:
The Apple Pay of Bitcoin?

development and operating costs on Qondado. Its fee policy just “keeps the lights on,” says Robles. He won’t give specifics about number of users so far, but adds “response has initially been very strong” to the company’s Facebook campaign.

‘There Is a Need’

But what kind of merchants are likely to accept Bitcoin? That’s what ISOs like Aliant are finding out. Brown says he’s targeting his base of high-risk merchants first, as these account for more than 60% of his base. He also expects card-not-present merchants to be among the first to sign on, since this is Aliant’s business focus.

But others, he hopes, will adopt Bitcoin. The first to sign up, indeed, was a plumbing contractor. As for takers overall so far, “We’re kicking out contracts,” Brown says.

To handle the back end of Bitcoin, Aliant has signed up NetCents Systems Ltd., a 5-year-old Vancouver, British Columbia-based exchange. For POS transactions, it’s relying on terminals from a Palo Alto, Calif.-based startup, Poynt Corp.

The Poynt device features an app library with business functions that go well beyond payment. The devices deployed by Aliant will work with a specialized connection to NetCents.

Pricing Bitcoin transactions could be tricky for Aliant, since there’s no interchange on which to base rates. Also, Brown says he wants to keep the service economical without attracting merchants that aren’t “serious” about accepting the digital currency.

Right now, Aliant’s Bitcoin transaction pricing ranges from 0.5% to just over 3%, with a fixed fee from a nickel up to 30 cents. The fixed fee

depends on volume, which brings it down, and risk, which does the opposite. There is also a monthly (\$9.95 to \$19.95) and annual (\$99) fee.

Other digital currencies could follow at Aliant. Brown says he is convinced “there is a need in the marketplace.”

A Means of Exchange

That may well be the case. On the face of it, there’s no reason merchants shouldn’t trade in Bitcoin every bit as much as they do in dollars, and no reason ISOs and processors shouldn’t enable this business. After all, as Qondado’s Robles says, “Bitcoin was designed to be a means of exchange.”

That’s on the face of it. Dig deeper, and you find volatility, cost, and network-scaling issues that raise big concerns. Chances are, these will be worked out. The question is how soon. **DT**

Bitcoin’s New Solution for Network Growth

Bitcoin’s heady rise last year has pleased investors and drawn the attention of derivatives exchanges and other institutional players, but it may also have obscured a development going on behind the scenes to solve one of the digital currency’s biggest drawbacks: its weakness as a payment method.

Bitcoin, which started out 2017 at a price just shy of \$1,000, was dancing above and below the \$18,000 mark in the first half of December. By mid-December, Bitcoin’s \$17,800 price placed the total value of all Bitcoin in circulation at close to \$300 billion.

Investor interest has been stoked not only by the currency’s meteoric rise but also by the implied endorsement coming from big-league futures exchanges. Chicago-based CME Group Inc. was set to start trading Bitcoin futures Dec. 18, but its crosstown rival, Cboe Global Markets Inc., beat it to the punch on Dec. 10. Both exchanges earlier received a green light for the contracts from the Commodity Futures Trading Commission.

But another event took place early last month that promises to clear up two key Bitcoin problems: network congestion and fast-rising transaction fees. Developers working on a project called the Lightning Network announced they had conducted a pair of successful live transactions using specifications they’ve been working on for more than a year.

While much work needs to be done, the transactions reportedly worked as expected across software prepared by different developers, according to Coindesk, a cryptocurrency news site.

For the past couple of years, the Bitcoin network has been plagued by slow transaction times and rising fees for users. Both problems are brought on by volume growth on an underlying blockchain limited by 1-megabyte blocks.

While some solutions attack the problem by increasing block capacity, Lightning proposes a bypass. It manages the transaction’s details via off-chain channels, broadcasting to the blockchain only when the transaction is culminated.

If Lightning is widely adopted, it could solve Bitcoin’s scaling problem, allowing for much faster growth and more reasonable transaction costs.

Fees are controlled by so-called miners, the organizations that create new Bitcoin by working out complex mathematical problems. As volume rises, miners can charge more to give a transaction a higher priority on the blockchain.

Bitcoin has already become a hot commodity for investors. Next up could be a solution that finally unlocks its potential as a payment instrument.



P2P And Beyond

Jim Daly

Suddenly, person-to-person payments services are gaining utility beyond just paying a person via a smart phone. What gives?

So you thought these newfangled person-to-person payment services were meant only to replace cash with smart-phone apps that enable individuals to send and receive money electronically? Think again.

All of a sudden, some P2P services are positioning themselves as payment alternatives for merchants. That's good news for companies like PayPal Holdings Inc., which finally may have found a profitable use for its popular but revenue-starved Venmo app.

It's also good news for Apple Inc. and its brand-new Apple Pay Cash service. Yes, Apple Pay Cash is primarily meant for individuals to pay each other on Apple mobile devices such as the iPhone, but it also can be used wherever the 3-year-old Apple Pay mobile-payment service is accepted.

That's really good news for Discover Financial Services, which is providing the network that will connect merchants to the Apple Pay Cash system. If consumers see Apple Pay Cash as a good way to buy things, Discover's transaction volume will rise.

If you're interested in cryptocurrencies, perhaps you're one of the lucky test subjects who can use the Square Cash P2P service from Square

Inc.—whose primary business is merchant acquiring and software services for businesses—to buy or sell Bitcoin.

Then there's Mastercard Inc. and its new Mastercard Cash Pick-Up service, which combines corporate disbursements with P2P. The recipient's money isn't electronically stored somewhere. It's spit out by an ATM as old-fashioned cash.

Monetizing Venmo

Jordan McKee, principal analyst, payments, at 451 Research LLC's Boston office, is watching all the P2P developments with satisfaction.

"It's an incredibly dynamic space at the moment, and it's fun to watch as the services evolve," he says.

McKee believes the services will need to keep on changing lest they lose customers who want more than a one-trick payments pony.

"It's going to be very unlikely that a consumer will continue to use an app that only sends money back and forth over time," McKee says. "The providers are starting to realize they need to evolve the value proposition."

Online P2P services, later supplemented by mobile iterations, have been around for about a decade, but the majority of consumers still haven't tried them, according to a recent 451

Research survey (chart, page 22). And no one has yet found a way to get consumers to pay for them, which in part explains the rush of new features.

PayPal clearly was hoping to generate a new revenue stream from merchants when chief executive Dan Schulman declared during the company's third-quarter earnings call in October that PayPal would begin "to monetize Venmo."

Venmo generated \$9.4 billion in payment volume in the third quarter, up 93% in a year. The service, however, charges no fees for sending funds from a Venmo balance, bank account, or debit or prepaid card. The only fee is 3% if funds come from a credit card, so, for all its popularity with consumers, Venmo contributes little to PayPal's top line.

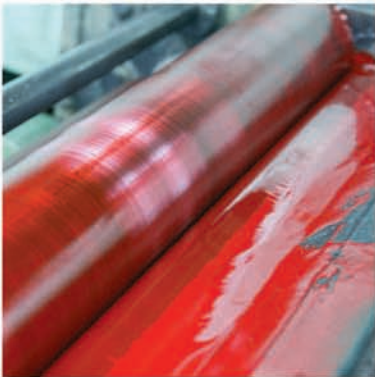
The first step in the monetization movement took place earlier in October with an announcement that as many as 2 million PayPal-accepting merchants were eligible to accept Venmo online and in-app. PayPal will collect the same merchant fees on these transactions as it does for regular PayPal payments. Those fees start at 2.9% plus 30 cents and decline with volume.

'A Huge Win for Discover'

Meanwhile, Apple is positioning the new Apple Pay Cash as an easy-to-use P2P service through its Messages app that sends and receives text messages.

single source for merchant supplies

profits direct to your bottom line



Flexible Billing Options

Inventory & Asset Management

Direct Ordering Via Phone or Web

Customized Printing & Manufacturing

Personalized Kitting & Distribution



GENERAL CREDIT FORMS, INC.

www.gcfinc.com • 888.GCF.NEWS

P2P App Usage

Daily
2.1%

Weekly
9.3%

Monthly
10.5%

Would
like to try
9.5%

Tried
once or
twice
13.2%

Never
55.3%

Note: 846 valid responses.

Source: 451 Research Voice of the Connected User Landscape Survey, third quarter 2017

The app gives Apple Pay Cash a social-networking overlay similar to that of Venmo.

Within Messages, users can send, receive, or request funds. The service also works with Apple Watch, and users can give instructions to Siri, Apple's artificial-intelligence exemplar, to issue funds.

Senders tap a digital-only Apple Pay Cash Card for the money, and may also rely on other cards stored in their Apple Pay wallet if sufficient funds aren't available on the Cash Card. The card is a prepaid product managed by Pasadena, Calif.-based prepaid card services provider Green Dot Corp. and its Green Dot Bank.

Recipients need an Apple Pay Cash Card to access funds. They can use the money instantly, unless a security check is needed, to pay someone or make purchases using Apple Pay in stores, apps, and on the Web, according to Apple. They also can transfer funds from Apple Pay Cash to their bank account.

While personal payments are the main market Apple is targeting, the Apple Pay Cash Card can be used for payments at any merchant that accepts Apple Pay, which relies on contactless near-field communication technology. Apple said in November that 5 million U.S. retail locations would be accepting Apple Pay at the

end of 2017, and that 67 of the top 100 U.S. retailers now take it.

Though the three so-called general-purpose "Pays"—Apple Pay, Alphabet Inc.'s Android Pay, and Samsung Electronics Co. Ltd.'s Samsung Pay—lag far behind PayPal in mobile volume, Apple Pay has been getting more usage than its two main competitors (chart, page 24).

Apple, without giving numbers, said Apple Pay users doubled over the past year and that transaction volume rose 330%. And now, Apple Pay Cash is poised to give the mother service a lift, though nobody knows yet how big that lift might be.

After all, why use an Apple Pay Cash Card rather than an account the consumer has in her Wallet to fund conventional Apple Pay transactions?

"I'm not entirely sure," says McKee of 451 Research. "If you're somebody who uses P2P services with some frequency and like the idea of a cash reserve, as we've seen with Venmo ... that's where I can see it."

In any case, Discover is poised to benefit from whatever merchant volume Apple Pay Cash generates because the transactions will go over its debit rails, presumably the Discover-owned Pulse debit network.

Mobile-payments consultant Richard K. Crone likens Apple Pay Cash

to a new tender type. "If you're introducing a new tender type, you need a network, you need processing rules, you need pricing, you need acceptance, and that's what Discover is providing for Apple Pay Cash," says Crone, chief executive of San Carlos, Calif.-based Crone Consulting LLC, who calls Apple Pay Cash "a huge win for Discover."

Discover will generate fee income when a customer pays a merchant with Apple Pay Cash because it reportedly will set the interchange rates merchants pay. But what the revenue arrangements are between it and Apple, such as whether Apple will get any of that interchange, is not publicly known. Discover referred questions to Cupertino, Calif.-based Apple, which declined comment.

Researcher McKee agrees that the Apple Pay Cash deal "is a massive win for Discover." He notes that Discover struck a deal in 2012 with PayPal, the online payments leader, to bring PayPal acceptance to the physical point of sale via Discover's merchant network, but nothing came of it.

Through its direct relationships with large merchants and agreements with numerous merchant acquirers that have made millions of small merchants Discover acceptors, Discover's

merchant base is now at or near parity with the Visa and Mastercard merchant networks.

“Discover is interested in leveraging its network in unique ways,” says McKee. “They’re very comfortable being that infrastructure in the background.”


Discover’s honeymoon with Apple might not last long, however. “Currently, the Apple Pay Cash Card is issued on the Discover network, but this is subject to change,” says a brief passage on the Apple Pay Cash terms-and-conditions page. Again, no elucidation from Apple.

Cold, Hard Cash

The Venmo and Apple developments show the potential of P2P services to be adapted for retail payments.

Mastercard’s new Cash Pick-Up service, in contrast, is aimed at underbanked or unbanked consumers. A transaction results in actual cash being dispensed from an ATM, not the movement of electronic money from one account to another.

The service enables consumers to pick up cash disbursements, including person-to-person payments or such payments as disaster-aid relief, social benefits, or rebates from companies, at ATMs without using a debit card. For senders, the service eliminates the need to cut checks or directly pay cash to recipients.



P2P is ‘an incredibly dynamic space at the moment.’

—Jordan McKee, principal analyst, payments, 451 Research LLC

A business or individual initiating a Mastercard Cash Pick-Up transaction creates a cash pick-up order, which alerts the sender’s bank to issue payment. A unique, four-digit PIN is sent to the recipient via text message in a matter of seconds. Upon entering the code into an enabled ATM, the recipient can retrieve the cash without using a card.

Fort Lee, N.J.-based Cross River Bank, Mastercard’s launch partner for the service, sees it as an addition to its payment services for business customers. In 2015, the bank worked with Mastercard on the launch of Mastercard Send, the card network’s near-real-time payment service.

“Part of Cross River Bank’s strategy is to be first to market with new payment types that can add value to

our clients,” Ben Isaacson, senior vice president and general manager of payments, says by email. “We’ve partnered with Mastercard to be very early to market on previous products like Mastercard Send, so it was a natural fit to start this dialogue.”

When it announced the program in September, Mastercard said it would test it in the fourth quarter with partners that included Payment Alliance International, the nation’s largest privately-held ATM provider. Mastercard is also working on making Cash Pick-Up available at ATMs located in stores across the country beginning this year.

The service initially is certified to run on ATMs manufactured by Hyosung and Genmega. Mastercard also teamed with Pin4, which has operated a similar cardless-disbursement system in Spain and Poland under the HalCash brand, to manage deployments.

Researcher Joseph Walent, associate director of the customer interaction advisory service at Maynard, Mass.-based Mercator Advisory Group Inc., says by email that Mastercard Cash Pick-Up is in line with developments Mercator has been tracking in countries such as Australia and India that involve sending a code to the recipient’s mobile device to retrieve cash from an ATM via a mobile app or online. But it’s the first



Its Apple Pay Cash networking deal ‘is a huge win for Discover.’

— Richard K. Crone, mobile-payments consultant

Digital Wallet Usage

Question: Which digital wallets, if any, have you used to make purchases with over the past 90 days? (multiple answers allowed)

PayPal	67.5%
Apple Pay	24.2%
Starbucks	15.0%
Android Pay	15.0%
Visa Checkout	11.0%
Chase Pay	7.7%
Samsung Pay	6.7%
Walmart Pay	6.4%
Dunkin' Donuts	6.1%
Capital One Wallet	4.3%
American Express Checkout	2.8%
Masterpass	2.5%
Kohl's Pay	1.8%
Wells Fargo Wallet	1.8%
Microsoft Wallet	0.3%
Other	1.5%

Note: 326 valid responses.

Source: 451 Research Voice of the Connected User Landscape Survey, third quarter 2017

one that also could involve the payment of wages, he says.

Also, the usage of PINs with text messages “allows for a wider audience when compared to the other mobile cash-access schemes that rely on either NFC or the quality of the resolution of the screen at the ATM to recognize a QR code,” Walent says. “That said, the use of a SMS text has been seen by some in the industry as a less-secure system with the possibility of intercept.”

Fraud, however, probably would be limited to daily ATM withdrawal levels, he adds.

Potential Battleground

Besides the old medium of cash, P2P services can now bring consumers into the new world of cryptocurrency. San Francisco-based Square in early December said it was expanding the Bitcoin pilot program it had launched a month earlier for what it said was

a “small” number of Square Cash users. The service under test is now being made available to an undisclosed number of additional users.

Square launched Square Cash in 2013 as a P2P payment service that allows users to send and receive money via debit cards.

The new Bitcoin feature allows users to buy and sell, but not send or receive, the digital currency. The test comes during a massive run-up in Bitcoin’s price that some observers are calling a classic bubble. From just under \$1,000 a year ago, the price soared to over \$17,000 in December, with most of the gains coming since August.

If the recent developments show that new utility can be added to P2P services, do they present a threat to the Big Daddy of P2P, Zelle, the service from bank-controlled Early Warning Services LLC?

Early Warning pegged Zelle’s payment volume at \$17.5 billion in the third quarter on 60 million transactions. Some 50 banks and credit unions are participating in the program, with 13 live as of late October, and 65,000 consumers were signing up daily, Early Warning said.

While Zelle clearly is gaining critical mass, the non-bank P2P providers, especially Apple, are showing they covet banks’ customers, according to analyst McKee.

“If I was a bank ... I would start to get pretty concerned at this point,” he says. “It appears Apple is trying to own more and more of the customer relationship.”

Apple certainly isn’t the only one trying to do that. Look for P2P to continue as a field of innovation—and a potential battleground. **DT**

—With additional reporting by John Stewart



ONLY ONE OF THESE BIRDS CAN
GIVE YOU THE LATEST NEWS
IMPACTING THE **PAYMENTS MARKET**

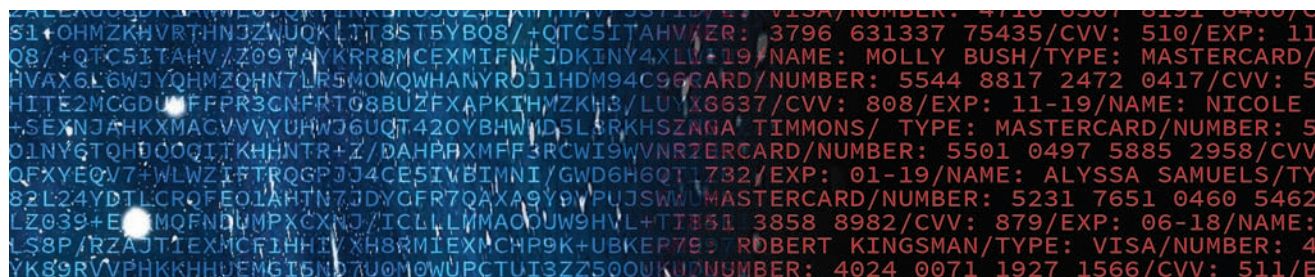
Today and every day follow

DIGITAL TRANSACTIONS

@DTPAYMENTNEWS on Twitter

DIGITAL
TRANSACTIONS
Trends in the Electronic Exchange of Value

WHATEVER HAPPENED TO ENCRYPTION?



Kmart, Arby's, Saks Fifth Avenue, Hyatt Hotels.

Those are just some of the merchants that reported data breaches in 2017. To be sure, 19% of U.S. merchants reported a hack last year, down from 22% a year earlier, according to Thales e-Security's 2017 Data Threat report. But being breached remains a catastrophic event.

Not only does a breach put millions of consumers at risk for fraud and identity theft, it is a public embarrassment for the breached company. Executives in the c-suite are certain to face questions from the media, the public, and investors about what steps they took to secure their customers' data.

If a merchant can't say it did everything possible to protect its database, the lapse can cause long-term damage to the company's brand.

The fallout can be so far-reaching that some merchants will try to keep the lid on a breach. That's what Uber did last year by paying hackers a \$100,000 ransom to delete stolen data—so the hackers said—rather than report the breach.

Arguably, one of the most effective ways to minimize the risk of a data breach is to encrypt all data moving over a network or stored, also known as data in motion and data at rest, respectively. At minimum, encryption, a process that translates data into a code that can only be read by someone with a decryption key, renders the stolen data useless if a breach occurs, unless the hacker can break the algorithm used to encrypt the data.

Since most hackers are looking for the path of least resistance, they are more likely to target merchants and other entities within the payment industry that don't encrypt cardholder data, data-security experts say.

False Sense of Security

Just one problem. As effective as encryption is, it is not that widely used by merchants and other companies that store or deal in payments data or other personally identifiable information.

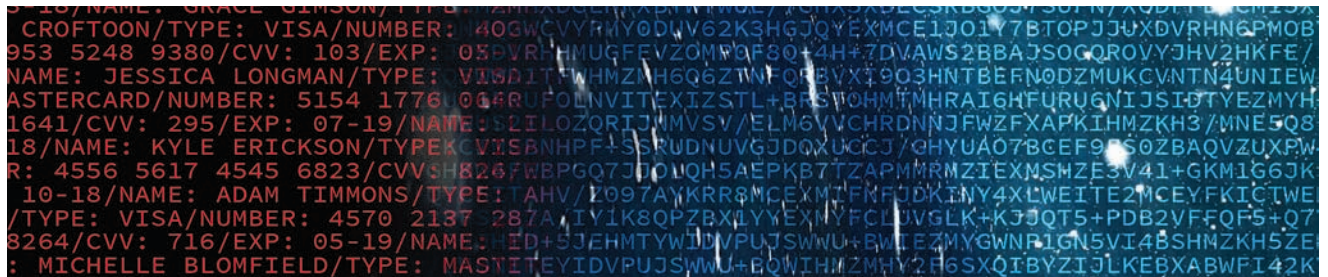
Even companies that manage massive storehouses of sensitive consumer data neglect to encrypt it. The huge credit-reporting concern Equifax Inc. shocked the nation last summer when, after hackers accessed 145.5 million records in its system, the company admitted it hadn't encrypted its data.

Why this neglect? After all, security experts have pushed encryption at least since the first major breaches were reported a dozen years ago.

The reasons are varied and complex. For merchants dealing with payment-related data, they include lack of education about the value of encrypting data and a need to make choices about how best to apply limited information-technology resources.

Widely touted as a potent data-masking tool, encryption has been slow to take hold in the payments industry, despite a continuing plague of data breaches. Here's what's going on to change that.

By Peter Lucas



There's also a false sense of security among merchants that compliance with the PCI Security Standards Council's main set of rules, the Payment Card Industry data-security standard, or PCI DSS, coupled with implementation of EMV-enabled terminals, is enough to protect card data.

"The misconceptions around encrypting card data and lack of inquisitiveness by the merchant community [are] slowing adoption," says Scott Dowty, chief revenue officer for Scottsdale, Ariz.-based payments technology provider Apriva LLC. "It's going to take merchants a long time to understand the importance of securing sensitive data."

Merchant Misconceptions

Although the merchant community has made strides securing data at rest through the use of tokenization, a process that replaces card data with a randomly generated sequence of numbers

and characters, it remains highly vulnerable to hackers targeting merchants' connections to processors. The reason? Data in motion is rarely encrypted.

A common misconception among merchants, according to security experts, is that as long as they are compliant with the PCI DSS, information leaving the point of sale and traveling to a processor for authorization is secure. The PCI DSS was created in 2004 to increase controls around cardholder data to reduce credit card fraud.

While the PCI DSS applies to all entities that store, process, or transmit cardholder data, it does not require data being transmitted over a private network, such as a connection between a merchant and a processor, to be encrypted. The standard's only encryption requirement concerns data sent over a public network.

In addition, it is not uncommon for merchants to believe that once they are validated as PCI-compliant, they remain so. The reality is that PCI com-

pliance is an ongoing process. A merchant can fall out of compliance at any time after being deemed compliant.

"Merchants have to be constantly performing PCI compliance, it's not just a one-time certification," says Edward "EJ" Jackson, head of security and fraud solutions for First Data Corp. "Becoming PCI compliant is a greater motivation for merchants than encrypting data that leaves their walls."

Another major misperception among merchants is that EMV chip cards will secure data cardholder data. The reality is that EMV was created to prevent fraud at the point of sale by authenticating the card to the POS terminal and vice versa.

As a result, any data passing from the EMV chip through a POS terminal and out over a network connection to a processor or gateway is vulnerable to hackers.

"The intent of EMV was not to solve data breaches, but to prevent fraud," says Wally Mlynarski, chief

BENEFITS OF P2PE

Makes account data unreadable by unauthorized parties

Devalues account data because it can't be abused—even if stolen

Simplifies compliance with PCI DSS

The P2PE Self-Assessment Questionnaire includes only 26 PCI DSS requirements

Offers a powerful, flexible solution

Source: PCI Security Standards Council

product officer for Atlanta-based processor Elavon.

Point to Point

To address the problem of securing data transmitted from a POS terminal beyond a merchant's walls, processors, acquirers, and payment gateways have begun touting point-to-point encryption, a process that encrypts data as it enters a card terminal and keeps the data encrypted until it reaches a secure endpoint where it can be safely decrypted.

Besides providing strong data protection, what makes point-to-point encryption appealing to merchants is that it significantly streamlines compliance with the PCI DSS. The PCI Security Standards Council says its P2PE self-assessment questionnaire (SAQ) includes only 26 questions, compared to more than 100 questions for its standard SAQ.

Some merchants can see an even larger reduction of self-assessment questions. Two Men And A Truck, a Lansing, Mich.-based moving company, has reduced the number of SAQ questions to about 20 for its franchisees, compared to more than 300, with the implementation of a point-to-point encryption solution from Bluefin, an Atlanta-based provider of payment security solutions, says Jake Gaitan, the company's IT director.

"We want to make sure that our franchisees can protect customer data, but we also wanted to find a way to alleviate the cumbersome

PCI-compliance process for them while still protecting customer data," Gaitlan says. "We don't want to be in the news for a data breach."

Two Men And A Truck began rolling out the Bluefin solution more than a year ago and now has more than 100 of its more than 400 franchisees up and running on it. In addition to providing strong data security starting at the point of sale, Bluefin's solution also enables Two Men And A Truck franchisees to securely accept card payments using mobile devices. Before, franchisees had to call in card numbers over the phone.

"Not having to pay the card-not-present rate is a savings for our franchisees," Gaitlan says.

Only PCI-certified P2PE solutions can be validated as meeting the security requirements of the PCI P2PE standard and listed on the PCI Council's Web site. Since some merchants are installing non-PCI certified P2PE solutions, the PCI Council issued guidelines in November 2016 to assist security assessors in evaluating non-PCI certified P2PE solutions against the PCI P2PE standard, and their impact on merchants' PCI DSS compliance.

The PCI Council says there is no guarantee that implementation of a non-PCI certified P2PE solution will streamline PCI compliance.

As of December, there were 45 PCI-certified P2PE solutions in the market, according to the PCI Security Standards Council's Web site. Certified solution providers include

terminal makers VeriFone Systems Inc. and Ingenico, FIS Payment Solutions, PayPal Holdings Inc. and Bluefin, which expected to have signed 60 processors and gateways to use its solution by the end of 2017.


Bluefin's platform encrypts all card data within a PCI-approved point-of-entry device and decrypts it offsite in a Bluefin hardware security module. After decrypting the data, Bluefin sends it to the processor or gateway for authorization.

The company began rolling out its P2PE solution in 2014, eight months after it received PCI certification. "Because we manage the encryption keys for merchants (including device key injection and decryption), this gives merchants the flexibility to go with any processor or gateway," says Rustin Miles, chief strategy officer for Bluefin, in an email message.

'A Complicated Matter'

One of the reasons for the dearth of certified P2PE solutions providers is that certification is a lengthy process that can take three to six months, and in some cases longer. "Certification is very complicated," says Apriva's Dowty.

One of the most time-consuming hurdles to certification, data-security experts say, is the extensive testing a P2PE solution must undergo. "Certification is less about the encryption technology and more about how the solution is managed and deployed,"



Innovative Integrated Payments for any Point of Sale



**EASY TRANSITION
TO US EMV**



**ALL US
PROCESSORS**



**RECURRING
REVENUE**



**INSTANT DEVICE
COMPATIBILITY**

Datacap's industry standard integrated payments solutions empower any Point of Sale, regardless of architecture, with the payments flexibility to accommodate any merchant. By writing to one simple interface, Point of Sale developers can keep pace with evolving trends and payment industry standards, so they can spend development dollars on POS innovation rather than payments.

With plenty of EMV experience in the US and Canadian markets, Datacap is the ideal partner for any Point of Sale provider in need of a comprehensive, processor and hardware agnostic integrated payments solution. Let's talk payments!



datacap
systems, inc.

© 2017 Datacap Systems, Inc. All rights reserved.

Get Started Today!

215.997.8989

datacapystems.com



says Bryan Thompson, chief technology officer for Beyond Inc., a Princeton, N.J.-based independent sales organization.

Having been an executive with Heartland Payment Systems when the acquirer suffered a data breach in 2008, Thompson is a strong proponent of P2PE because it addresses the need for encryption when the transaction is initiated, which provides more control over the data assets on the front end.

After Heartland's data breach, the company's chief executive at the time, Robert Carr, pushed for implementation of end-to-end encryption

(E2EE). Similar to point-to-point encryption in that data is encrypted at the point where a transaction is initiated, end-to-end encryption varies from P2PE in that the data remains encrypted all the way through the last mile to the card networks.

A P2PE solution, on the other hand, encrypts data before it reaches the merchant's gateway provider or processor, which then flows the data, encrypted or decrypted, through a secured pipeline to the networks. In other words, the back-end pipes carrying the data are secured, but the data itself is not necessarily encrypted.

"The reason Heartland could implement end-to-end encryption is that it owned the technology deployed from the merchant to the card brand," says Thompson. "With point-to-point encryption, the data is encrypted from the merchant up through the front door, which is the processor or gateway."

While P2PE does not encrypt data from the start to the finish of a transaction, Thompson is quick to point out that once a gateway or processor decrypts the data, it resides in a secure environment before moving further downstream in the payments ecosystem.

A RANDOM APPROACH TO DATA SECURITY

Encryption may provide a strong defense, but it's only as good as the math behind it. A criminal with better math skills, or a more sophisticated decryption application, can crack the algorithm used to encrypt data.

That possibility is what has some data-security experts concerned that encryption won't be enough in the future to deter hackers. One stronger data-security solution would be to create random combinations of numbers and letters to scramble data, they argue.

"No matter how complex a cryptographic cipher is, it has an underlying pattern that can be discovered and reverse-engineered to unscramble the data," says Gideon Samid, chief technology officer for the digital currency BitMint and the "Security Notes" columnist for *Digital Transactions*. "With quantum

computing on the horizon, the threat to data security is growing exponentially."

Quantum computers are powerful machines built on the principles of quantum mechanics and capable of solving problems in minutes that require years for today's computers. IBM Corp. says it expects quantum computing to lead to breakthroughs in the fields of medicine, financial services, artificial intelligence, and supply chain and logistics. Unfortunately, it could also create breakthroughs for criminals looking to beat data encryption, Samid says.

Randomness, on the other hand, applies a theory of quantum mechanics that all events are truly random. Ciphers built on randomness do not use mathematics and therefore have no underlying patterns that can be discovered.

"Cracking ciphers is not easy, but the payments industry does need to lay the foundation to support new, stronger forms of data security," says Wally Mlynarski, chief product officer for Elavon. "The process has started with the use of dynamic payment credentials and tokenization."

While some payments experts believe that the introduction of randomly created ciphers is five to 10 years off, the big question is whether merchants will be fully on board with using ciphers to protect data by then.

"A lot of executives in the c-suite view cryptography as a black box, something that's so complex it's essentially a mystery to them," Samid says.

If the top decision makers in a company don't understand encryption and its variants, they

are less likely to embrace it, Samid adds.

Executives' perception of encryption is starting to change, however, as insurance companies educate merchants about the threat to consumer data and the value of strong cybersecurity, says Mlynarski.

Despite many merchants' lack of urgency when it comes to encrypting card data, payments experts agree that the worst thing the payments industry can do when it comes to data security is to stand pat.

"There are powerful data-security solutions that are used in government that will begin trickling down for commercial use and help raise the level of data security for the public," says Scott Dowty, chief revenue officer for Apriva. "Data security must evolve, because there is a shelf life to encryption."

“It’s hard to replicate what Heartland did with end-to-end encryption because of the need for an entity to control all the technology assets from front- to back-end,” Thompson says. “The further data travels away from the merchant before being decrypted the less vulnerable it is. Encryption should carry throughout the entire payments ecosystem, but it’s a complicated matter.”

Nevertheless, P2PE is still a potent tool for merchants to thwart hackers, Thompson says. Beyond, which is headed by Carr, plans to have its P2PE solution PCI-certified.

Indeed, the PCI Council states in its blog that merchants are only responsible for protecting card data in their own environment, not that of the payment gateway or processor.

“With that, it follows that there’s no additional scope reduction benefit from implementing an E2EE solution over a P2PE solution, and any data loss following transmission to a gateway/processor would be the legal responsibility of that gateway/processor, not the merchant,” the blog says.

‘Tug of War’

Despite the benefits of P2PE, its implementation still poses challenges for merchants, as many of the solutions are specific to the type of POS device deployed.

Some processors, such as First Data Corp., developed P2PE solutions for their own branded terminals first, and are working next to develop solutions for other makers’ models. First Data has rolled out a P2PE application for its Clover line of terminals, of which about 700,000 have been deployed.

One drawback to developing device-specific solutions, payments experts say, is that each solution must undergo certification. That, and the time it takes for the device to receive a PCI certification, are among the factors that have slowed merchant adoption of P2PE, payments experts agree.

The good news for merchants is that, unless they are using exceptionally old devices—which is unlikely, as the EMV mandate has forced upgrades across the entire spectrum of merchants—legacy equipment can be reused. Merchants simply need to inject the encryption keys for a P2PE solution into the

device’s software, says Thompson.

While PCI-certified P2PE solutions are considered by some merchants to be the gold standard, some payments solution providers are forging ahead with making P2PE a standard feature of their payment applications. Some of these providers are awaiting PCI certification.

N1 Merrick Bank[®]
Merchant Acquiring

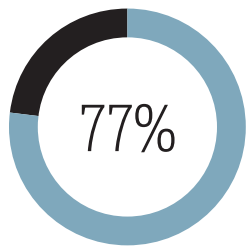
Portability • Profitability • Personalization

*Taking
ISO Sponsorship
to the
next level*

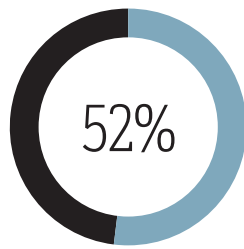
Meet us at:
NEAA
Jan. 29 -31, 2018
Mohegan Sun Casino, CT

www.MerrickBankAcquiring.com

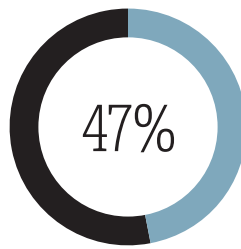
DATA SECURITY FAST FACTS



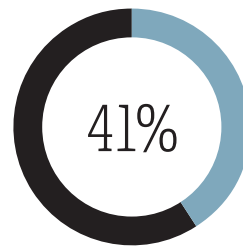
77% of retail respondents planned to increase security spending in 2017, up from 61% in 2016



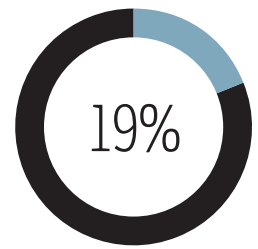
52% of U.S. retailers have been breached at some point



47% of U.S. retailers rank best practices as their top data-security spending driver



41% of U.S. retailers rank data-security compliance as a top spending driver



19% of U.S. retailers feel "very" or "extremely" vulnerable to security threats

Source: 2017 Thales Data Threat Report, Retail Edition

Elavon, for example, has begun rolling P2PE into all its merchant solutions. "We are shifting all our products to where P2PE will be included," Mlynarski says.

Elavon is in the final stages of having its P2PE solution PCI-certified. The company already has a component of the solution PCI P2PE-validated.

North American Bancard is another solutions provider rolling out a P2PE solution. The Troy, Mich.-based payments-solutions provider is concentrating its initial P2PE efforts on the medical-merchant community.

"The need to encrypt customer payment data is further ahead in the medical category than it is in retail because of HIPAA," says Jim Parkinson, chief information officer for North American Bancard. HIPAA is a government mandate regulating health-care information.

One potential drawback to using a non-PCI-certified P2PE solution is that, if a data breach occurs, it could open the merchant to criticism that it did not do everything possible to protect its data.

"How the technology is sold is a big component of any new security technology," says Dowty. "There are players in the market also selling end-

to-end encryption solutions and non-PCI-certified point-to-point encryption solutions, and that's creating a tug of war over what's the best option.

"For merchants, the value proposition of any non-PCI-certified encryption solution is going to be whether it is the best solution available," Dowty continues. "But there is a lot of value to merchants in a PCI certification."

'A Game of Leapfrog'

The last speed bump to merchant adoption is an age-old complaint of merchants, that the card companies' penchant for rolling out new mandates requiring the upgrading of terminals, such as EMV, is siphoning off valuable IT resources that could be redirected to implementing P2PE.

"There is definitely a frustration among our members that EMV compliance is pulling more resources that could be used for more effective data security," says a spokesperson for the Washington, D.C.-based National Retail Federation. "Data security is a game of leapfrog. Build a 10-foot wall and the hackers will come back with a 12-foot ladder. EMV still sends card data in the clear."

Although Beyond's Carr agrees that EMV has sucked up a lot of merchants' IT resources, he adds that EMV implementation represents an opportunity for merchants to strengthen their data security by adding P2PE and tokenization for data at rest.

But if data security truly is a game of leapfrog, it raises the question whether the slow rate of P2PE adoption is giving criminals time to develop new ways to reverse-engineer the coding that scrambles the data so they can get at the actual card information (box, page 30).

"There is no question that P2PE needs to evolve," says Dowty. "But for that to happen everyone (merchants, processors, acquirers and gateway) needs to get on the same page."

For all the optimism about how P2PE will close a gaping hole in merchants' data-security defenses, the greatest challenge to adoption remains the lack of merchant awareness.

"We don't get a lot of merchants asking about P2PE," concedes Parkinson. "Education about the value proposition for P2PE is going to be the key."

Without that education, many of the misconceptions that are confusing merchants about encryption will persist. **DT**

THE ONLY MAGAZINE COVERING THE TOTAL PAYMENTS MARKET

In 2015, there were 131.2 billion digital transactions in North America.

Digital Transactions magazine covered them all.

It is the only publication addressing the total market.

Financial institutions, independent sales organizations (credit and debit ISOs, ATM deployers and value added resellers), processors, along with the top tier retailers all turn to *Digital Transactions* for the trends affecting the payments market and, more importantly, their livelihoods.

Covering the electronic payments business for 13 years, *Digital Transactions* magazine is your independent source for changes affecting the payments market. *Digital Transactions* is also available in a digital edition on our web site, DigitalTransactions.net

Subscribe today by going to Bolandhill.omega.com/dtr/ to start tackling the ever-changing payments market.





Are We There Yet?

Kevin Woodward

What's happened to the e-commerce checkout and why it isn't easier to make a payment.

Instant access is the byword for online retailers. It's what online shoppers want all the time and what e-retailers strive to provide so their consumers can buy when they want. Epitomizing that is a frictionless checkout experience, one that makes it painless to authenticate and authorize the payment.

But that ideal type of checkout remains just that, an ideal. While e-commerce is now in the midst of its third decade of widespread availability since the deployment of the first Web browser, issues surrounding the online checkout process abound.

"Too often, merchants see consumers get all the way through the funnel to add items to their carts, but then leave their sites without checking out," says Arnold Goldberg, vice president of merchant product and technology at San Jose, Calif.-based PayPal Holdings Inc. "Why? Oftentimes it's because the checkout process is filled with friction. Customer have to type in user names, passwords, credit or debit card information, shipping and billing addresses, and if they don't have their card information on hand, or can't remember their password, that can result in an abandoned cart."

The urgency and necessity for dealing with the online checkout

experience is clear. E-commerce sales comprised 9.1% of all U.S. retail sales in the third quarter of 2017, says the Census Bureau of the Department of Commerce. That's up from 8.2% in the same quarter of 2016. In three years, e-commerce sales are expected to total \$708 billion, according to Javelin Strategy & Research.

The Changing Consumer

The effects of this growth are rampant. Traditional malls are struggling as big-name retailers close stores and consolidate locations. Some retailers have closed up entirely as the challenges posed by merchants with more astute online-sales methods hammered them.

At the root is the changing consumer. With smart phones and tablets found in most households—77% of U.S. consumers have a smart phone, the Pew Research Center says—shoppers are used to researching, finding, and comparing prices from the comfort and convenience of wherever they are using the device in hand.

That expectation of easy shopping access extends to how they pay. Few consumers want to enter a 16-digit credit card number, a card verification code, billing and shipping addresses, and related information on a smart-phone screen.

Consider that e-commerce platform provider Mobify, in its Monthly Mobile Commerce Benchmarks for 2017, noted that in October, the latest month with available data, the average conversion rate on a desktop computer was 5.9% for average order values between \$100 and \$175. That compares to 4.3% for tablets and 1.9% for phones. Orders of less than \$100 and more than \$175 share a similar pattern.

"Consumers are moving to mobile as their primary computing device, and at the same time, expect instant access to the things they want and need at the point of discovery," says Goldberg. "Because of this, retailers can no longer wait for customers to come to them."

The phenomenon is putting extra pressure on merchants and their payments providers to find ways to expedite the checkout process.

"Clunky checkout drives up what I call [the] 'insult rate,'" says Andy Barker, senior director of strategy and growth for global payments at Magento Inc., a major e-commerce platform provider based in Campbell, Calif. "One of the worst things to do when a customer is handing you money is to look at them and say, 'That's not good enough,'" Barker says.

Difficult mobile-commerce checkout experiences also will drive down conversion rates, encouraging consumers to shop elsewhere with easier checkout processes.

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.

AMERICAN EXPRESS
GLOBAL MERCHANT SERVICES

AMERICAN EXPRESS NO LONGER SETS THE RATE.

With OptBlue, the rate is up to you or your processor. And this kind of flexibility can help you close the deal with Merchants and offer even better service.

Learn More

Just hear what Merchants have to say:

"We got back to our service provider quickly, and we ask for our rates to be reviewed based on our volume. We did find the right American Express rate for our business."

—Robin's Candy, Great Barrington, MA

OptBlue

The leader in POS just took another step forward (and another)

Introducing TWO new software packages:

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.

Harbortouch Salon & Spa

Harbortouch Salon & Spa expands the Free POS Program to a vast new market, with industry-specific features like appointment setting, waitlist management, multi-station support and email/text reminders.

Harbortouch's Free POS Program is unparalleled in terms of the cost to the merchant, the quality and functionality of the POS system, and the compensation to the sales partner. Not to mention, our training and support are second to none. If you aren't already offering Harbortouch POS, there has never been a better time to start!

Email 1500@harbortouch.com to get started or visit www.harpogram.com

*Terms & conditions apply. Please contact Harbortouch for complete details. © 2016 Harbortouch Payments, LLC. All rights reserved.

ingenico GROUP

Your Complete Guide to Payment Security / PCI, P2PE, and more

Watch Webinar & View SlideShare

*"PCI DSS" is an acronym in the payments industry that is commonly discussed yet is often misunderstood. Watch this recorded webinar: PCI in the POS / What's New, What's Next, and What Merchants Can Do to Simplify Compliance to finally gain a clear understanding of the Payments Compliance Industry Data Security Standard and its latest updates. Our payment security experts answer frequently asked questions such as:

- What is PCI DSS?
- Why do merchants need to comply?
- What changes are in the latest PCI DSS version?
- What can merchants do to make the compliance process easier?
- How can P2PE, EMV and tokenization enhance payment security?
- And more...

Watch Webinar & View SlideShare

TOP 3 WAYS to Grow Your Opportunities with BlueStar

Download the PDF Starter Kit and avoid leaving money on the counter.

Today's mobile solutions with integrated peripherals make it easier than ever to add revenue within your existing client base. Let BlueStar show you how

PDF GET THE KIT

What's included:

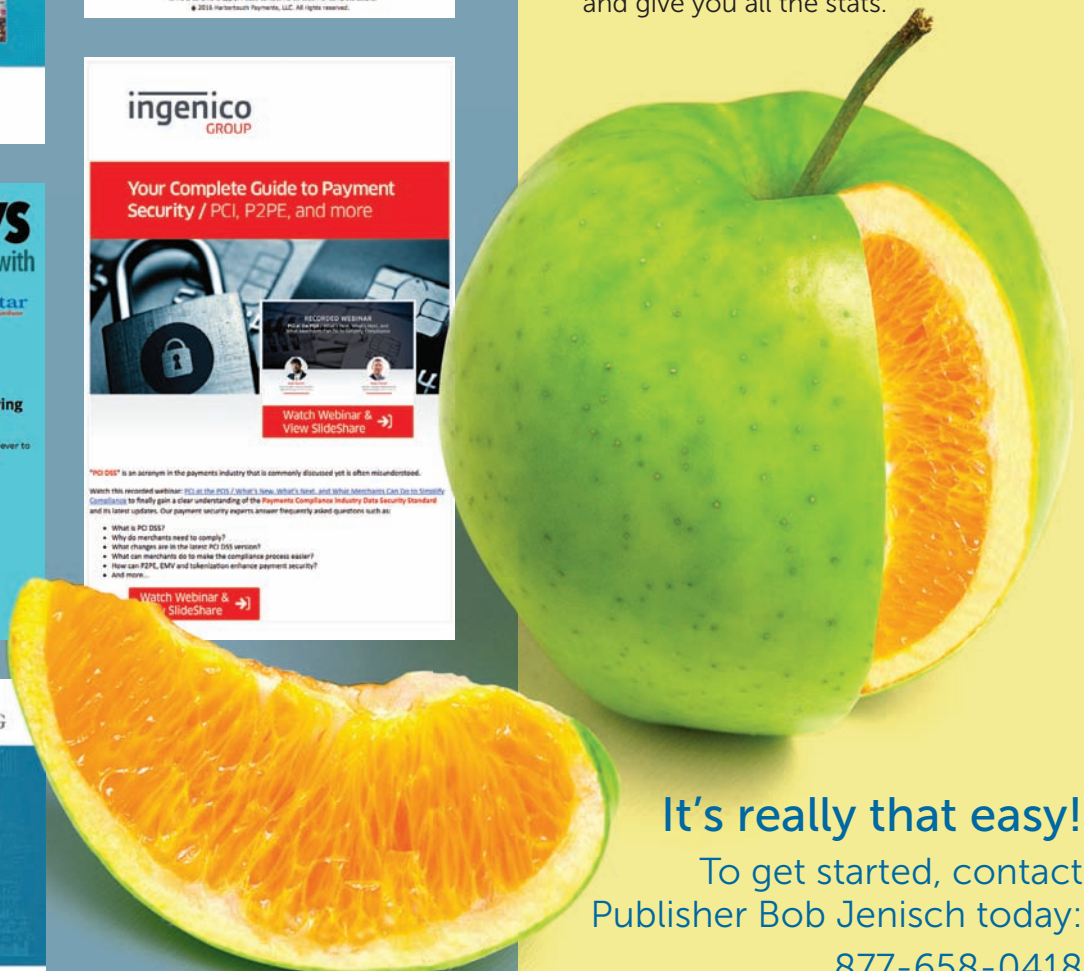
1. The Top 3 Business Growth Opportunities
2. Steps to Obtain a Reseller License
3. Areas to Expand in the Marketplace

elevate | FUNDING

No credit checks.
No application fees.
Ever.

Direct access to underwriters.
Syndication opportunities.
ACH or credit card splits.

www.elevatefunding.biz



It's really that easy!

To get started, contact Publisher Bob Jenisch today:

877-658-0418

bob@digitaltransactions.net

Making consumers complete forms at checkout is one of the biggest issues in e-commerce, says Richard Btaiche, product manager at Shopify Inc., an Ottawa, Ontario-based e-commerce platform and payments provider.

“The majority of online buyers are still spending a lot of time fumbling around forms,” Btaiche says. “Any distraction or notification could prevent customers from completing their purchases, so the longer it takes to check out the more chances of distraction.”

Profit Vs. Security

Why isn't the online checkout experience easier, especially years after the introduction of e-commerce to the United States? Chalk that up to a payment card system built for face-to-face transactions, where authentication procedures were designed with the customer present.

Though much more sophisticated today, the U.S. payments system favors profit over security, says Suresh Dakshina, president of Chargeback Gurus, a McKinney, Texas-based chargeback-management company.

Certainly, security is important, but the tradeoff is that to make a payment service very secure usually requires stringent authentication measures, ones that many retailers

are not willing to impose because they may prevent more legitimate sales than fraudulent ones. Many retailers are willing to accept some fraud loss in expectation they will make up the costs with more legitimate transactions.

In Europe, for example, many markets opt for more security, Dakshina says. “Most of them do not have one-click purchase because they have made it understood that [consumers] have to go through multiple authorizations,” says Dakshina. Still, though the online checkout experience continues to create friction, the expectation is to make it as smooth as possible. In other markets, the expectation and what consumers may have become accustomed to could differ, he says. “Europe is more security-oriented. We are more profit-oriented.”

The prospect of chargebacks is a serious issue for online merchants. Efforts to reduce chargebacks may require better authentication methods. A seemingly legitimate transaction may actually be a bad one that produces a chargeback when, for example, the actual customer discovers his card data was misappropriated for a transaction.

For U.S. merchants, especially, chargebacks are an expensive repercussion of accepting online payments, says Barker. “They need more payment methods that guarantee payment,” he says. “We see fewer chargebacks in Europe and Asia because those markets rely on more bank-based

methods than the U.S., which is largely credit-based.”

As Shopify's Btaiche says, “Merchants expect that a frictionless buying experience does not come at the expense of reduced security for the customer or themselves. It should be working for them, and against the fraudsters.”

Seamless Checkout

What merchants, and consumers, want is as easy a checkout experience as possible. The question is what does that look like. For some, Uber, the ride-sharing service that requires no discrete action to complete a payment, is the goal. Others desire an even smoother experience.

“The ideal checkout is no checkout at all,” says Barker. In December, Magento introduced Instant Purchase, its one-click checkout process. For merchants, Instant Purchase offers a customizable button, a mobile-optimized process that Magento says reduces time-to-purchase by 90% and offers automatic shipping to the shopper's default address, along with support for multiple payment methods.

“We're moving in a direction where the customer doesn't have to do anything but say, ‘I want this,’ and they get it,” he says. “There are challenges to overcome, but the Internet of Things is getting us closer to this point with technologies like Amazon Echo and Google Home.”

Amazon Echo and Google Home are in-home devices that use voice assistants to help consumers make purchases and retrieve information such as the weather forecast and movie times.

In Barker's view, the next wave of checkout innovation is finding a way for merchants to secure stored payment details. That's especially critical in a time when data breaches are rife.

“We can't get rid of the actual payment transaction, but we need to utilize technologies to make it almost invisible,” he says. “Smoother, faster, and more secure.” Magento's service

‘Too often, merchants see consumers get all the way through the funnel ... but then leave their sites without checking out.’

—ARNOLD GOLDBERG, VICE PRESIDENT OF MERCHANT PRODUCT AND TECHNOLOGY, PAYPAL HOLDINGS INC.



arrives following the 2017 expiration of Amazon.com Inc.'s one-click payment patent.

Tokenization, the technology that replaces the actual card data with a randomized sequence, "which makes it so that consumer payment credentials are never released to the end merchant," is a major part of this, he says.

Shopify's Btaiche echoes Barker. "Our thoughts on the ideal checkout is not a faster or better checkout, but rather no checkout at all," he says. Shopify Pay, an accelerated payment service for Shopify merchants, decreases the checkout process from 16 steps to one, he says, adding, "It has increased the conversion rate by up to 18% for returning customers." Shopify Pay saves pertinent consumer shipping and payment details and can be used at participating e-retailers.

PayPal struck out on its own prior to the Amazon patent expiration with its One Touch checkout service. Launched in 2014, One Touch has more than 70 million global users who don't have to type in a username, password, or payment information after the initial setup.

"The less data fields a consumer has to fill out, the more likely it is that they will actually convert," says PayPal's Goldberg. "Consumers expect seamless access to the products and services they want and need—and

when there's too much friction in the way they will abandon their cart and go to an e-commerce or m-commerce site that lets them [have] seamless checkout."

Working on It

Payments companies can help merchants with this. One way is the coming implementations of 3-D Secure 2.0, an authentication protocol that sends more data to issuers without intruding into the checkout experience as the prior version did.

"3-D Secure 2.0 is designed to minimize the interaction required with the cardholder, thereby reducing overall transaction friction while still increasing transaction security," Btaiche says. "The vast majority of transactions will be completely seamless and transparent, but transactions which require additional authentication will be able to leverage tools such as the native biometric capabilities of the device to authenticate the customer and the transaction."

Another initiative that may affect the online checkout is the work of the Web Payments Working Group, an industrywide standards-develop-

'Our thoughts on the ideal checkout is not a faster or better checkout, but rather no checkout at all.'

—RICHARD BTAICHE,
PRODUCT MANAGER,
SHOPIFY INC.



ment organization that is part of the World Wide Web Consortium. The W3C, with U.S. headquarters in Cambridge, Mass., develops protocols and guidelines for the Web.

The working group, which includes 157 individuals and 60 organizations, is "doing important work around standardizing how people pay on the Web," says Btaiche. Shopify is one of the participating organizations. "People's online buying habits are evolving, and so must payment providers," he says.

With the changing nature of online shopping, and with smart phones proliferating and consumer expectations increasing, a smoother, faster process is necessary. "The challenge for merchants is to allow customers to shop and pay for products in a way that mimics the touch and feel of the brick-and-mortar experience," says Magento's Barker. "Consumers increasingly want the endless aisle, or line busting where they would rather just take the product and get billed later rather than fuss with the payment logistics."

Is the time of the frictionless checkout at hand? Perhaps not next year, but payments and e-commerce providers are working on it. **DT**

'Clunky checkout drives up what I call [the] "insult rate."'

—ANDY BARKER, SENIOR DIRECTOR OF STRATEGY AND GROWTH FOR GLOBAL PAYMENTS, MAGENTO INC.



PIN on Glass broadens the digitization of payments worldwide. Many even think it could have an impact on gross domestic product in certain countries.

Why PIN on Glass Is the Next Big Thing



Sam Shawki is chief executive and cofounder of MagicCube, Santa Clara, Calif.

The key to higher acceptance rates for cards, lower fees for merchants, and better security lies in moving the point of sale from hardware to software, says Sam Shawki.

There is no doubt that the continued progress in moving to digital forms of transactions has made a big impact on the global economy. There is also no doubt that the key to helping push this move further is on the acceptance side.

After all, if your local merchant or mom-and-pop store only accepts cash, there is nothing you can do other than pay in cash. Many small and medium-size businesses and individual contractors only accept cash or checks. In fact, the U.S. remains behind Europe when it comes to moving away from checks, and in many other countries, even larger merchants only accept cash. While there are many reasons why certain segments of merchants do not accept cards, one big reason is the unjustifiable cost the merchant has to endure. Case in point: 55% of small businesses in the U.S. still don't accept credit cards.

If the payments industry is ever going to achieve its lofty goal of nearly doubling global card acceptance from 47 million to more than 90 million devices by 2020, it's clear that reducing the cost of acceptance is exactly how we will get there.

Moving away from hardware is crucial to such a transformation. Think of it this way: In an era where everything is virtualized and downloadable, why do we still have to contend with arcane, specialized devices to accept payments? As with my Nikon camera and my Sony CD player, acceptance devices from the

likes of Ingenico, VeriFone, and even Square will eventually disappear and be replaced with mobile apps.

As is usually the case in business, the move from hardware to software in payments is gradual. It started with Square, iZettle, PayPal Here, and so on. But one big obstacle to getting to a downloadable point-of-sale acceptance device that you and I can use is the fact that the keypad that's used to enter your PIN remains a hardware requirement. While PIN usage is still limited in the United States, it's a requirement in most of the world, and the U.S. is expected to move in this direction.

Three Key Benefits

Enter PIN on Glass technology, which transforms regular mobile devices into full-featured POS systems capable of securely accepting payment card PINs on a touchscreen. PIN on Glass stands to revolutionize retail payments for merchants and financial institutions as it improves transactional security, lowers the cost of card acceptance, and increases card-acceptance rates.

Also, by enabling higher credit card acceptance rates for consumers and lowering costs for merchants, PIN on Glass offers a societal benefit. It broadens the digitization of payments worldwide. Many even think that PIN on Glass could have an impact on gross domestic product in certain countries.



Digital Transactions News

We deliver the payments industry news to your email inbox daily!

Digital Transactions News is packed with news and information from the \$123.4 billion transaction industry:

- ▶ Two original stories every issue
- ▶ Trending stories, so you know what our subscribers are reading
- ▶ Links to Digital Transactions magazine
- ▶ Calendar of events
- ▶ **PLUS!** "In Other News" The most complete listing of announcements from the payments community

Subscribe today at Bolandhill.omeda.com/dtr/
or email publisher Bob Jenisch at Bob@digitaltransactions.net



Here are three key benefits that PIN on Glass technology brings to consumers, merchants, and banks alike:

1. Better security for consumers.

The reality is, PIN technology is far more secure than relying on a signature. For example: Fraudsters can easily use lost or stolen EMV cards when a signature is used as a verification method, and merchants are unable to decline an untrusted transaction if it's been approved with signature verification.

2. Affordable card acceptance costs for merchants.

Since PIN on Glass doesn't require merchants to purchase expensive, dedicated payment terminals and instead leverages existing, regular mobile devices, the technology significantly lowers the cost of card acceptance. That's a critical factor in coaxing more small businesses to accept credit cards rather than continue to rely on cash and checks.

3. Greater payment volume for banks.

PIN on Glass offers banks that issue EMV debit and credit cards lower POS fraud costs, higher purchase volumes, and increased merchant demand for EMV PIN at POS. Furthermore, EMV PIN solves for lost and stolen card fraud, addresses merchant demand that

EMV be enabled for PIN, and lowers the cost of acceptance for merchants, which in turn boosts payment volume on bank-issued payment cards.

By replacing the need for hardware-secure elements to build, deploy, and remotely provision and manage POS systems and other Internet-of-Things devices, a software-based approach to payments is capable of impacting our entire economy by enabling growing businesses to more easily join the digital age.

Specifically, a software-based approach can offer mobile-screen security and protection of data entry and financial PINs with or without a secure card reader. And where card readers aren't required, it can enable secure tap-and-pay applications.

A software-based approach can also allow for operating-system security for next-generation POS systems that replace the need for expensive security chips and eliminate the headache of updating entire operating systems for POS device vendors. In addition, it enables remote monitoring and over-the-air upgrades across the board.

Doing away with single-purpose, proprietary POS systems and embracing the unique capabilities of a software-based approach to payments

will increase payment networks' transactional volumes, allowing the entire payments ecosystem to grow unencumbered by the constraints of costly, legacy POS systems.

A pitfall that we are worried about is that when we move to software, there are other, lower-security techniques, like white-box encryption, that can meet some of the new standards. We worry that some may go this route. This can impede the move to software and cause concerns.

PCI Gets on Board

Luckily the PCI Security Standards Council, of which we, and many of you, are members, has embraced a software-based approach to payments. A full draft of relevant PCI requirements will be finalized in the next few months. The specifications put a framework in place that will allow the right technologies to start coming to market and get adopted.

The key to strengthening mobile commerce is improving acceptance at the point of sale. Acceptance rates will only improve if we begin to move beyond the proprietary, legacy, hardware-device model and embrace software capable of downloading fully-featured POS systems into any off-the-shelf mobile device. **DT**

ADVERTISER INDEX

Aliant Payments	888-638-6103	www.aliantpayments.com	Page 7
Datacap Systems	215-997-8989	www.datacapsystems.com	Page 29
Digital Transactions	877-658-0418	www.digitaltransactions.net	Pages 25, 33, 35, 39
Electronic Merchant Systems	866-887-8907	www.emsagent.com	Inside Back Cover
eProcessing Network	800-296-4810	www.eprocessingnetwork.com	Page 17
General Credit Forms	888-GCF-NEWS	www.gcfinc.com	Page 21
Harbortouch	800-201-0461	www.isoprogram.com	Page 1
Humboldt Merchant Services	877-457-4479	www.hbms.com	Back Cover
MagTek	562-546-6467	www.magtek.com	Page 3
Merrick Bank	800-267-2256	www.merrickbankacquiring.com	Page 31
PAX	877-859-0099	www.pax.us	Page 5
PaySafe	281-583-4400	processing.paysafe.com	Page 15
ProPay, a TSYS Company	888-227-9856	www.propay.com	Inside Front Cover
USAePay	866-490-0042	www.usaepay.com	Page 9

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.



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.



AGENT

866.887.8907
www.emsagent.com



NEED A HIGH-RISK PARTNER? LOOK TO HUMBOLDT BEFORE YOU LEAP.

Tired of payment processors leaving you out in the cold just because you're a so-called "high-risk" merchant? Fortunately, Humboldt Merchant Services has been providing industry-leading solutions to hard-to-place merchants since 1992. Solutions like in-depth access to fraud and chargeback materials the very next business day after a claim is filed by an issuing bank. Plus, in-house Risk Assessment and Underwriting Departments for faster and easier approvals. No wonder Humboldt Merchant Services has been offering hard-to-place merchants a perfect landing spot since 1992.

**JOIN THE 25-YEAR
INDUSTRY LEADER TODAY.
877.457.4479 | HBMS.COM**



Boutique Client Experience



Multi-Currency Conversion



Specialized Chargeback Reporting



Full Suite of Anti-Fraud Services

INDUSTRIES WE SPECIALIZE IN:

Adult Content • Extended Warranty • Direct Marketing • Free Trial Billing • Nutraceuticals • CNP Tobacco
Dating • Business Opportunity • Buying Clubs • Firearms & Ammunition • E-Cigarettes • Bail Bond Issuers

