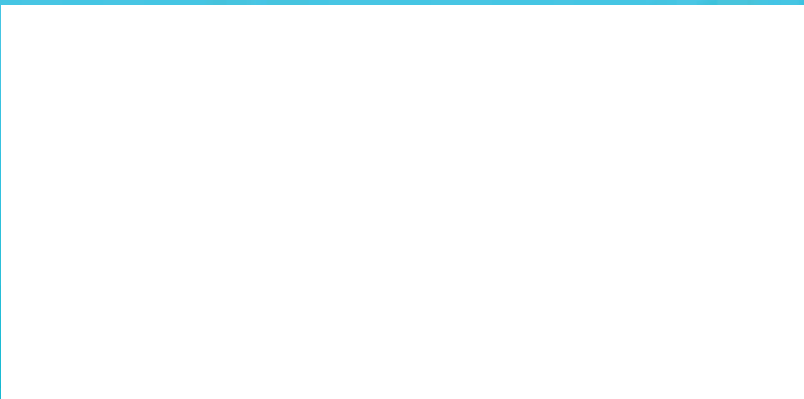


DIGITAL TRANSACTIONS

Trends in the Electronic Exchange of Value

FISERV'S BIG BITE

Its \$22-billion megamerger agreement with First Data sets it up to be a dominant player on both the bank and merchant sides of payments. How will the industry react?



ALSO IN THIS ISSUE

- ✦ Kroger's Wallet Strategy
- ✦ PayPal's Busy Agenda
- ✦ PCI And Card Theft
- ✦ Where Crypto Is Vulnerable



Your Payment Partner of Choice



A920

E500

A80

Aries 8

Smart Retail Solutions



PAXSTORE

PAX's modern and secure Advance Management Platform for partners and developers to utilize with the PAX Smart Retail Solutions.

www.paxstore.us



PAX

www.pax.us

+1-877-859-0099

© 2019 PAX Technology Limited. All Rights Reserved. PAX's name and PAX's logo are registered trademarks of PAX Technology Limited. All other products or services mentioned in this advertisement are trademarks, service marks, registered trademarks or registered service marks of their respective owners.

Let Us Teach You POS!



Join Harbortouch on our Training Road Show!

As point-of-sale systems become a more integral part of any payments portfolio, it is more critical than ever to become an expert on POS! Join Harbortouch as we hit the road and offer free POS training around the country this spring. There is NO COST for this training, and you do not need to be a current Harbortouch partner to attend.

Topics covered will include:

- POS Sales Strategies
- POS Software
- Features & Benefits
- POS Hardware

By the end of the training, you will be a POS expert ready to attack the competition and build a lucrative integrated payments portfolio!

2019 TRAINING ROAD SHOW DATES:



LOS ANGELES, CA
LOS ANGELES
AIRPORT MARRIOTT
APRIL 29 - MAY 2



NEWARK, NJ
CROWNE PLAZA
NEWARK AIRPORT
MAY 5 - MAY 9



CHICAGO, IL
FOUR POINTS BY SHERATON
CHICAGO O'HARE AIRPORT
MAY 12 - MAY 16

Why Learn POS?
Better Accounts - Higher Margins - Lower Attrition

To register, please visit www.harbortouchroadshow.com



HARBORTOUCH[®]
A SHIFT4 COMPANY

'[Fiserv] looked in the past [at acquiring merchant processors], but the multiples were always too high. This is seen as their payments play. It's been coming for a long time.'

PAGE 20



CONTENTS

March 2019 ■ Volume 16, Number 3

20 Fiserv's Big Bite

Its \$22-billion megamerger agreement with First Data sets it up to be a dominant player on both the bank and merchant sides of payments. How will the industry react?

4 The Gimlet Eye

The Tech Imperative

6 Trends & Tactics

Kroger Takes the Proprietary Route in Mobile Payments

The grocery giant has launched a digital wallet—and added its own debit card.

Does Cash Need Legal Protection in Stores?

That's the question as some governmental entities start to require that stores accept greenbacks.

A Look at EMV's Headway in 2018

Over two-thirds of U.S. card-accepting merchant locations were capable of accepting chip cards in December, Visa's latest report card says.

P2P Payments Prove Pokey for Many People

For all the buzz around real-time transfers, not all P2P payment users are taking advantage of that capability.

Plus, Security Notes proposes a digital currency you can hold in your hand.

14 Acquiring

Near Field Or Quick Response?

As if the payments business wasn't enough of an alphabet soup, QR codes are now vying with NFC for dominance in mobile payments. Which technology will win out at the point of sale?

26 Strategies

So Many Irons in the Fire

PayPal's octopus-like strategy covers everything from P2P payments, bill pay, and the point of sale to parting ways with eBay. Can Schulman and Co. keep all the balls in the air?

32 Security

PCI's Latest Security Gambit

New software standards aim to resolve—or at least minimize—credit card theft. There's cause for both optimism and caution.

34 Security

Cryptocurrency's Weakest Links

To purloin crypto, hackers are importing successful—and very familiar—methods from the world of fiat money. Here's what experts say needs to be done.

39 Endpoint

PayPal: Secrets of a Relentlessly Relevant Juggernaut

Staying on top in payments requires close attention to a few ironclad rules, say Saurabh Wahi and Davis Ward.

Cover illustration: Jason Smith, Fotolia.com

A Better Way To Experience Banking

Providing faster more convenient solutions with everything you need in hardware, software and services.



Security

Access account information beyond the teller line with faster more engaging solutions in the palm of your hands.



Showcasing solutions at GNECU



Versatility

The DynaPro Go is a mobile encrypting device that provides convenience, offering all the payment methods in the market today.



Authentication

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



FIND OUT MORE ▶

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



The Tech Imperative

When news broke in mid-January that Fiserv Inc. had offered to buy First Data Corp. in an all-stock transaction, we knew instantly we had our cover story. The trouble was, our February issue was already buttoned up, so we knew we'd have to wait for March.

As often happens, this turned out to be a blessing of sorts. The intervening weeks gave us a chance to reach more sources and gather more data as people moved past their immediate shock and began figuring out the transaction's many angles. In the meantime, we also were able to chronicle the announcement as well as the developing story behind it in our daily newsletter, *Digital Transactions News* (sign up at our Web site if you're not receiving it).

What gripped people immediately was the sheer scope of the deal and the fact that the buyer is, of all entities, Fiserv, rather than another merchant processor. Well, as it happens, the \$22-billion offering price is pretty big, bigger even than the 2017 deal in which Vantiv Inc. swallowed Britain's Worldpay, but it's not necessarily the biggest processor deal of all time.

That distinction may well go to another transaction involving First Data. That was Kohlberg Kravis Roberts & Co.'s \$29-billion leveraged buyout of the company in 2007. That price looms even larger today. After 12 years of inflation, it's more like \$36 billion in 2019 dollars.

More interesting than the identity of the buyer and the price, though, is the why of this deal. What source after source told us is that the critical importance of technology, and its dizzying pace of change, is such that payments companies have to find a way to either develop it fast or acquire it—and keep ahead of rivals doing the same thing.

That requires resources that can often come only through acquisitions, sometimes sizable ones. The bigger the deal, after all, the harder it is for competitors to catch up. This is true across a broad front in this business, from point-of-sale systems to integrated payments to peer-to-peer transfers to bill payment to faster payments to cryptocurrency. It embraces new fields like the Internet of Things, cashierless checkouts, and experiential e-commerce.

The result of this tech binge, according to many we talked to, is that we can expect more big mergers, perhaps including some on the scale of Fiserv-First Data. It won't be easy, and it won't come cheap, and it will surely reshape the payments landscape. Even if Fiserv-First Data falls apart—it requires regulatory and shareholder approvals—other big transactions are sure to come, probably sooner than later. It's in the nature of the industry now.

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, x7

bmitchell@digitaltransactions.net

Rob Akert, 877-658-0418, x6

rakert@digitaltransactions.net

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

John Stewart, Managing Director

Robert A. Jenisch, Managing Director

For advertising information, call 877-658-0418.

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

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 © 2019 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.



THE PLATFORM FOR ALL YOUR PAYMENT PROCESSING NEEDS

PAYMENT PROCESSING

ACH, CHECK AND
CARD PAYMENT
RAILS

TENS OF BILLIONS
Payments Processed Annually

TREASURY AUTOMATION

TREASURY WORK-FLOW
AUTOMATION, API'S,
SDK'S AND SAMPLE UI'S

-45%
In AR Days-Outstanding

PLATFORM SECURITY

ADVANCED MONITORING,
FRAUD PREVENTION
AND RISK TOOLS

100,000+
Locations

The iStream payments platform, Pymntz™ is centered around
Payments, Data, A/R, A/P, Treasury Management and Reconciliation.

Utilization of iStream for payment processing for both bank and card centric transactions, requires no changes to existing banking relationships, resulting in **decreased costs, increased revenue, all from a single provider.**



TRENDS & TACTICS

Kroger Takes the Proprietary Route in Mobile Payments

Grocery-store giant The Kroger Co. is joining the ranks of retailers with a proprietary mobile-payments service, and adding a debit card to boot.

Cincinnati-based Kroger, which has 2,800 stores under numerous banners, last month unveiled Kroger Pay and its accompanying Kroger Rewards debit card. Kroger Pay, available for iOS and Android mobile devices, uses quick-response codes instead of the near-field communication contactless technology employed by general-purpose mobile-pay services such as Apple Pay and Google Pay, which Kroger does not accept.

The new program includes digital coupons and personalized offers. In Kroger's case, the loyalty program also is tied to a new debit card, dubbed "Rewards." Consumers accrue loyalty points when using Kroger Pay and can receive additional points when the payment method is the Rewards debit card or a general-purpose prepaid card that also carries a Kroger store brand.

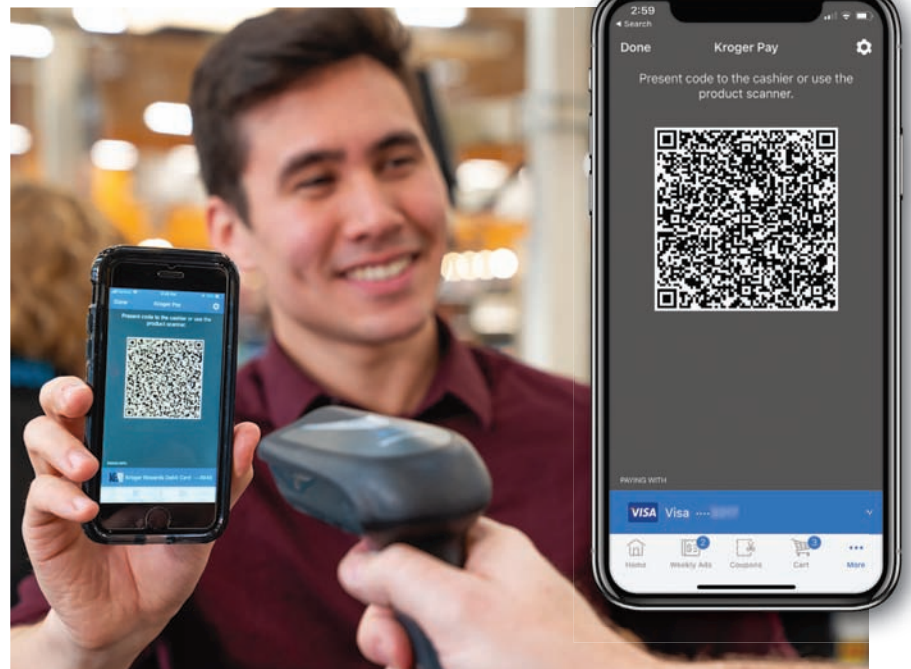
Kroger Pay also works with other credit, debit, and prepaid cards. While Kroger Pay does not lock out general-purpose payment cards, it offers incentives to use its own card. Currently,

Kroger Pay is available in Columbus, Ohio, with plans for nationwide expansion later this year.

Kroger Pay generates a one-time-use QR code in the app that sends payment information to the point-of-sale system via a scan. To use Kroger Pay at the checkout, the user opens the app in her smart phone and selects Kroger Pay from the "More" menu. She then either enters a PIN or scans a biometric. The QR code is scanned,

followed by scans of items to purchase. At a self-checkout station, the consumer taps "Mobile Pay" on the POS system and follows the prompts.

Many merchants choose QR-code technology for their own mobile-pay services because it can be an easier integration into the checkout process, where consumers and employees are used to scanning, and it may enable some transactions to sidestep the payment networks.



A consumer holds a Kroger Pay-generated QR code for a cashier to scan.

(Photo: Kroger Co.)

For example, Target Corp.'s Wallet only works with Target's debit card, credit card, or the Target Mastercard. The general-purpose mobile wallets, such as Apple Pay, Google Pay, and Samsung Pay, accept multiple payment types and work with multiple retailers if NFC technology is activated on their POS terminals. NFC is a wireless technology that some retailers have eschewed, but many others, including Target, have eventually adopted.

NFC also presents a better consumer experience, says Thad Peterson, senior analyst at Boston-based Aite Group LLC.

For example, to use Kroger Pay, the consumer has to find and open the Kroger app, then "find the QR code and present it," Peterson tells *Digital Transactions*. "There's more friction in their solution than there is using Apple Pay." Apple Pay only requires the consumer to hold the iPhone or Apple Watch near the contactless reader to complete a transaction.

The question for the consumer then becomes, is there enough incentive in the loyalty program to use a QR code and overcome the purchase friction, Peterson says.

Kroger did not respond to a *Digital Transactions* request for comment. But the company has been more than willing to take high-profile stands on payment issues in the past. In 2016, it sued Visa Inc. over the routing of EMV debit card transactions. That suit is in settlement talks, according to recent court filings.

Last summer, Kroger's Foods Co chain in California began boycotting Visa credit cards, citing high acceptance costs. Neither Visa nor Kroger would comment about the boycott, including whether it's still on.

—Kevin Woodward

Does Cash Need Legal Protection in Stores?

Efforts to ban cashless stores are afoot in New Jersey and some of the nation's largest cities, including New York. But does cash really need legal protection from payment cards and mobile wallets?

That's the question public officials as well as payments and retail executives are mulling. Opponents of cashless stores say businesses that require customers to use credit or debit cards or mobile payments are shutting out consumers who may not have access to those payment forms.

A mid-February report released by a New York City Council committee says 11.7% of the city's households are unbanked compared with 7.7% for the U.S., and 25.1% of city households are underbanked versus the nation's 20%.

"The unequal impact of cashless policies is cause for concern," the report says. "While the technology

provides a range of benefits for business owners, relying solely on cashless payments generates a segregated purchasing system. This policy poses great harm for certain parts of the populations, and statistics show that this is disproportionately felt by poor, marginalized and vulnerable communities."

The Council is considering two proposed ordinances pertaining to cash usage. One would ban retailers and restaurants from refusing to accept cash. First-time violators could be subject to a fine of \$250, with \$500 fines for subsequent violations. The other would permit cashless stores but require owners to post clear signage about their payment policy.

The Philadelphia City Council on Feb. 14 passed an ordinance that would prohibit most stores from refusing to accept cash or charging cash-paying customers a higher price, according to

RESIDUAL STREAM BUYOUTS

ISOS - AGENTS - SAAS - ISVS

THE CUTTER ADVANTAGE:

No Minimum, No Maximum Transaction Size
Work with all Major Processors
Team of Subject Matter Experts Providing Superior Valuations
Highest Ranking Satisfaction based on Seller Feedback
Advantageous Referral Program

Denise Shomo | 610.451.4096
denises@cutterfinancial.com

Alex Daily | 615.663.5088
alex.d@cutterfinancial.com

Katelyn Neiman | 484.638.6802
katelyn@cutterfinancial.com



Philly.com, a news site affiliated with *The Philadelphia Inquirer*. The measure went to Mayor Jim Kenney for his signature. Another pro-cash measure is pending in Washington, D.C., according to press reports.

The National Retail Federation questions the need for legislation to protect cash from its electronic enemies.

“Retailers are not going cashless,” J. Craig Shearman, vice president for government affairs public relations at the Washington-based trade group, tells *Digital Transactions* by email. “The retail industry as a whole welcomes cash and most likely will for years to come. The examples of retailers turning down cash are very

few and isolated, and usually involve specific circumstances.”

But Bruce Wayne Renard, executive director of The National ATM Council Inc., says the Jacksonville, Fla.-based trade group of ATM deployers and suppliers supports the recent proposals.

“There is a significant portion of America’s population that are unbanked or underbanked, making most or all of their daily payments using cash,” Renard says in an email. “These citizens, typically in lower socio-economic strata, should not be locked out of access to goods and services simply because they don’t have a credit card or mobile wallet to make

a purchase. There is a basic ‘fairness/non-discrimination’ aspect to businesses not accepting cash, and this is what’s at the heart of the local and state legislation that has surfaced of late in our major cities.”

A New Jersey bill that would ban stores from banning cash at the point of sale recently passed both houses of the state Legislature by overwhelming margins and was awaiting Gov. Phil Murphy’s signature in mid-February. A spokesperson in the governor’s office wouldn’t say if he would sign it. If enacted, New Jersey would join Massachusetts as the only states to protect cash payments in stores.

—Jim Daly

A Look at EMV’s Headway in 2018

Its biggest growth years might be over, but the EMV chip card standard continued to make headway in the U.S. last year.

The number of U.S. merchant locations accepting EMV chip cards grew nearly 15% in 2018 while Visa EMV payment transactions rose 27%, according to recent data from Visa Inc.

In its latest report on the conversion of general-purpose card payments from magnetic stripes to EMV chips, Visa says 3.1 million U.S. card-accepting merchant locations, or 68% of the total, could process EMV cards in December 2018, up about 400,000 locations from 2.7 million a year earlier (chart). The chip-card-accepting merchant base was little changed from September’s 67% rate, but well above the 59% rate in late 2017.

Some 511.1 million, or 71%, of Visa-branded cards now have chips. That’s an increase of 6% from 481.8 million cards in December 2017. Visa says 297.5 million of its debit cards

A U.S. EMV Snapshot

	Dec. 2018	Dec. 2017	Change	% Change
Accepting merchant locations (millions)	3.1	2.7	0.4	14.8%
% of accepting storefronts	68%	59%		
Visa chip cards (millions)	511.1	481.8	29.3	6.1%
Credit	213.6	209.1	4.5	2.2%
Debit	297.5	272.7	24.8	9.1%
% of total cards	71%	67%		
Chip payment volume (billions)	\$88.9	\$78.0	\$10.9	14.0%
Chip transactions (billions)	1.9	1.5	0.4	26.7%
% of Visa payment volume on chip cards	98%	96%		

Source: Visa, *Digital Transactions*

and 213.6 million of its credit cards are now EMV-enabled.

Payment volume on Visa chip cards totaled \$88.9 billion in December, up 14% from \$78 billion a year earlier. The EMV transaction count jumped nearly 27% to 1.9 billion. Visa

defines a fully-enabled merchant location as one where 75% of card-present payments are chip-on-chip: an EMV card read by an EMV-enabled point-of-sale terminal.

The main purpose of the EMV conversion was to thwart counterfeit

IS YOUR ISO AS IMPORTANT TO YOUR PROCESSOR AS IT IS TO YOU?



IF NOT, LET'S TALK AT SEAA

STOP BY OUR BOOTH AT SEAA OR CONTACT
ROSS PAUP
ROSS.PAUP@FIRST-AMERICAN.NET

SCOTT DEFAZIO
SCOTT.DEFAZIO@FIRST-AMERICAN.NET

Why partner with First American Payment Systems?

- Award-winning customer service
- Industry leading account management team
- Best-in-class business management dashboard
- Custom contract, ISV, and integration capabilities
- Multiple front-end access, proprietary back-end, and electronic onboarding

Dedicated Account Management
Multiple Gateway Solutions
Real-time Account Alerts
Full Product Suite

Same-day Approvals
Next Day Funding
1stPayMobile
1stPayPOS Pro

www.first-american.net/iso-partnerships

Copyright © 2019 First American Payment Systems, L.P. All rights reserved. First American Payment Systems, L.P. is a registered ISO of Fifth Third Bank, Cincinnati, OH and is a registered ISO of Wells Fargo Bank, N.A. Concord, CA



fraud, to which mag-stripe cards are highly vulnerable. For merchants that accept EMV cards, dollars lost to counterfeit fraud as of September were down by 80% from September 2015's losses, Visa says. Counterfeit fraud losses for all merchants were down 48%.

The EMV conversion officially began in October 2015 when the major card networks imposed, over the protests of many retailers, liability shifts that forced merchants to absorb financial losses from counterfeit fraud if their POS terminals couldn't accept chip cards. Previously issuers largely bore the brunt of counterfeit fraud. EMV's big growth years were 2015, 2016, and 2017 in the wake of the liability shifts.

Now fraudsters are migrating to other channels, including online commerce and account takeovers ("Batting the Bots," December, 2018).

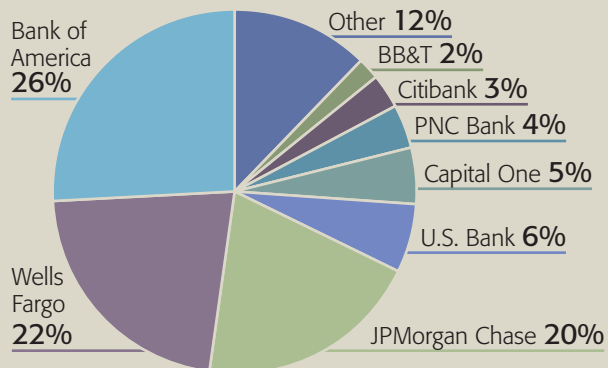
Next up in the EMV conversion is the retrofitting of fuel pumps at gas stations for chip card acceptance. After getting a three-year reprieve from the networks due to the complexity and cost of upgrading their pumps, gas stations face their own liability shift in 2020 ("The Expensive Fuel-Pump EMV Retrofit," November, 2018).

—Jim Daly

P2P Payments Prove Pokey for Many People

Where Zelle Gets Its Users

(Question: What bank do you use to access your Zelle account?)



Note: 258 respondents.

Source: Aite Group

Speed is a key selling point for person-to-person payments, but many P2P users aren't taking advantage of real-time payment capabilities offered by their providers, according to findings from Aite Group LLC.

Answers from 693 consumers who had used a digital P2P account to receive money in the 12 months ending in 2017's fourth quarter show that 53% of respondents said they were able to use funds within 30 minutes or less of reception. That includes some 11% of respondents who said they had their funds in less than a minute and 18% claiming funds were available in one to five minutes.

Still, many consumers reported funds availability took 24 hours or more.

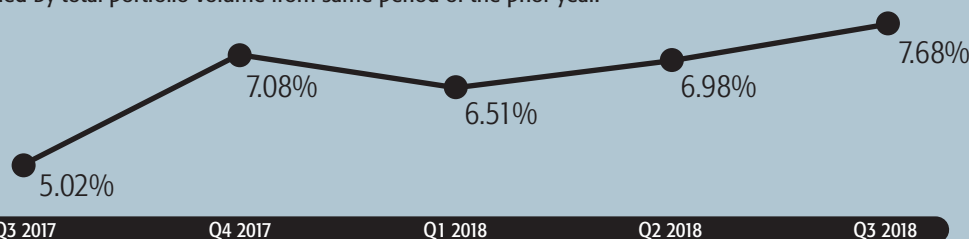
"With real-time payments capability becoming a common offering among providers, a surprising 25% of U.S. consumers who have used their digital P2P payment account in the last 12 months report it took more than one day to receive a digital P2P payment," says the new report by Talie Baker, a senior analyst at the Boston-based research firm. "This indicates that a large portion of U.S. consumers are not making full use of the real-time payment capability offered by their provider."

Some P2P services, including the bank-controlled Zelle and Facebook Inc.'s Messenger, don't charge for real-time payments. Others do, however, including PayPal Holdings Inc.

MONTHLY MERCHANT METRIC

Growth in Same-Store Sales Year Over Year

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



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

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

Source: The Strawhecker Group © Copyright 2019. The Strawhecker Group. All Rights Reserved. All information as available.



and the PayPal-owned Venmo service, according to Aite.

“Sixty-eight percent of U.S. consumers who used Facebook Messenger to receive payments in the previous 12 months and 79% of U.S. consumers who used Zelle to receive payments in the previous 12 months reported receiving payments in 30 minutes or less,” the report says. “By comparison, just 41% of U.S. consumers who used PayPal to receive payments in the

previous 12 months and 49% of U.S. consumers who used Venmo to receive payments in the previous 12 months report receiving payments in 30 minutes or less. More than 20% of U.S. consumers who used PayPal or Venmo in the previous 12 months to receive payments report it took more than one day to receive a payment.”

San Jose, Calif.-based PayPal is working to generate revenues from P2P transactions, which historically

have been free to consumers (“So Many Irons in the Fire,” page 26). With Venmo, for example, the company charges consumers for instant transfers, and more merchants are paying to accept the service.

In other findings from the wide-ranging study, Aite says Bank of America Corp. is the leading financial institution consumers use to access a Zelle account. Some 26% of 258 respondents with a bank-provided Zelle account said they used BofA to access Zelle. Not far behind were Wells Fargo & Co. and JPMorgan Chase & Co. (chart, page 10).

The study is based on two surveys. One, commissioned by Visa Inc., surveyed 2,078 consumers in late 2017. In the other, Aite surveyed 2,538 consumers who received funds disbursements between June 2017 and May 2018. **DT**

—Jim Daly

CORRECTION

In “The SRC Express,” January, the last paragraph on page 31, continuing onto page 32, is not correct. It should have read as follows:

For example, network rules concerning tokens could interfere with merchants’ freedom to route debit transactions to the network of their choice, argues the MAG’s Townsend, if the rules prevent outside networks from receiving access to the full set of security control validation and PAN data in the detokenization response provided by the payment network.

Digital Transactions regrets the error.

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™

1(800) 296-4810

eProcessingNetwork.com



© eProcessing Network, LLC. All Rights Reserved. All trademarks are the property of their respective holders.

Re-Materializing Digital Money



Gideon Samid • *Gideon@BitMint.com*

Minting money has become a mouse click in the Federal Reserve's computer. Ninety percent of circulated funds is never materialized in either coins or bank notes. And the recent craze for cryptocurrencies further cements the de-materialization of money.

The advantages of digital currency are clear and numerous: it stores on a pinhead; it is paid with the speed of light; it is minted in a jiffy; it may be made traceable and taxable. Alas, de-materialized money lacks the sense of assurance projected by a pack of \$100 bills, a silver coin, or a gold bar.

Indeed, de-materialized money is a juicy target for counterfeiting. It also shakes our sense of privacy, and—most alarming—it depends on uninterrupted cloud services. Emergency planners are horrified at the thought of a network collapse that would invalidate the financial grid, with devastating consequences.

Is there a way to keep the overwhelming advantages of digital money while holding on to the salient advantage of metal coins?

Yes. Allow me to introduce chemical digital money, or re-materialized cyber currency. It comes in three types. Type I is a hybrid coin. Electronic money is stored in a micro SD chip, which in turn is fitted into a chemical shell that must be cracked like an eggshell to pull the micro SD (and the money) out.

The value of the digital money inside the coin is marked on the shell. If the shell is intact, the payee can be sure the micro SD was not tampered with, and so will accept the materialized coin for its face value. The holder of this hybrid coin can always crack the shell, and read the MicroSD to his phone to use the money digitally. More features and details appear in publications describing US Patent #9,471,906.

Type II (or "RockCoin") is based on a new technology recently published by Case Western Reserve University (Samid and Wnek: "The Rock of Randomness.") This concept involves using modern 3D printing technology to construct a "rock" as a randomized combination of seeded

composite plastics that projects a data signature in response to applying the rock to electro-chemical measurements.

Using this technology, the Fed can mint physical coins in any denomination, however large. The minted rock will come with a marked ID and a designated face value. The public ledger will also publish the coin's signature.

What happens when the holder of this coin passes it as payment? The payee will fit the coin into a simple and commonplace RockCoin-Verifier, apply the electro-chemical test, and confirm that the rock is indeed the minted coin of the declared denomination.

Today's level of scientific knowledge does not allow us to mint this electro-chemical rock per order. In other words, we have no way to manufacture a coin that would comply with given measurements. The mint has no idea, in advance, of how the measurements will read. That means that no counterfeiter can take coin measurements specified in the public ledger and build a compliant rock. Which in turn means that if a rock reads as the public ledger says it should, then it is 100% the real thing.

In one fell swoop, society can maintain a payment regime even if terrorists or a natural catastrophe have brought the Internet down. Each coin verifier will hold its own copy of the public ledger. So now we are back into cash mode, only now the fundamental advantages of digital money are intact. Since all the circulating coins are identified, they can be taxed. And they can be suspended, or even invalidated if the authorities suspect misuse or foul play.

RockCoins can come with expiration dates, and certain coins may include their custodial history. Privacy may be taken to the maximum, perhaps on small denominations, and to the minimum on large coins.

Using the BitMint money language, the RockCoin can be parceled out to tradable claim checks, which are purely digital. Much like a quarter or a dime, the RockCoin is robust and handy. Coins will vary in size, shape, weight, and color.

Type III? That posits use of the rock technology over the shell of a hybrid coin.

One thing is clear. Payment continuity is a must for survival. Purely digital finance is vulnerable to evil-doers and unfortunate mishaps. Chemical digital money may be the only thing between us and societal chaos. ■

Simplifying Payments
...to simplify your life.



EVO MAKES IT EASY FOR YOU TO BE SUCCESSFUL.

Unlike other processors, we'll build a relationship with you, invest in you, and provide the support and resources every partner needs:

- An entire team that will follow up on leads and close sales for you
- Fast, easy onboarding of your MIDs
- Generous residuals paid on-time each month
- Omni-channel payment solutions
- Responsive service and 24/7 tech support for your merchants

EVO DOES IT ALL FOR YOU.

LEARN MORE.

VISIT: EVOpayments.cc/simplify | **CALL:** 855.795.0635



Near Field Or Quick Response?

Kevin Woodward

As if the payments business wasn't enough of an alphabet soup, QR codes are now vying with NFC for dominance in mobile payments. Which technology will win out at the point of sale?

In the United States, unlike many other parts of the world, near-field communication has been the favored technology for linking mobile wallets to point-of-sale equipment. And NFC may be almost assuredly on the cusp of adding to its U.S. dominance.

But with the arrival in the U.S. market of China's huge Alipay wallet and its technology based on Quick Response codes, it may be imprudent to dismiss QR systems as a basis for mobile payments.

The two technologies are engaged in a see-saw battle worldwide. Depending on the day of the week, payments professionals may think that mobile-payments services using NFC are taking over the industry, while on another day it may appear that Quick Response codes are positioned to dominate.

That could be easy to assume, given that QR code-based payments are favored by tech giants Ant Financial Services Group, parent of Alipay, and WeChat, operator of WeChat Pay, both of which are used by millions of Chinese consumers, with merchant acceptance expanding around the world ("China Calling," September 2018).

At the same time, though, NFC technology appears to be dominant,

especially in developed markets where Apple Pay, Google Pay, Samsung Pay (collectively known as the "Pays"), and contactless cards are widely used.

Reinforcing that idea is that U.S. banks and credit unions are about to issue millions of contactless EMV cards that will use NFC connectivity to communicate with POS terminals. Visa Inc. expects more than 100 million such cards in issue by the end of 2019.

In the United States, at least, the distinction between NFC and QR codes generally depends on whether the mobile-payment service is designed for a single merchant or for multiple merchants.

Typically, the retailer mobile wallets favor QR codes for their proprietary systems. That's because they can control these wallets, incorporating payment methods that can be less expensive than the card networks or that entice consumers to share more shopping information. The most recent entrant is the big grocery chain Kroger Co., which rolled out its own rewards-laden mobile wallet last month.

Other examples include the Kohl's Pay app from retailer Kohl's Inc., which requires a Kohl's charge card.

Still others, like the highly popular mobile-payments service from Starbucks Corp., demand that consumers load funds into the app, though they can choose from a variety of sources, even Apple Pay and Chase Pay, the JPMorgan Chase & Co. service.

'Very Excited'

Generally, NFC works best where there exist networks supporting general-purpose card brands. "NFC is the solution for the world that is built on network payments," says Thad Peterson, senior analyst at Boston-based Aite Group LLC.

"It is well-suited to markets that are primarily network-based, such as the United States," he adds. "I say that because NFC is a linear extension of the existing infrastructure." On the contrary, QR codes exist where there aren't network-based systems, he says. "They don't require a central processing network to run."

In 2018, 84% of North American smart phones supported NFC technology, says ScientiaMobile Inc., a Reston, Va.-based mobile-device intelligence firm. By 2020, 2.2 billion NFC-enabled handsets will be online globally, says the NFC Forum, a Wakefield, Mass.-based trade organization.

NFC, which is an essential technology in the payments industry but unknown to most consumers, has distinct advantages and use cases where it makes sense. It also stands to gain

even more advantages as dual-interface cards with contact and contactless EMV capability enter the U.S. market.

The next generation of dual-interface cards—contactless cards based on magnetic-stripe technology were introduced in the mid-2000s but failed to catch on—stands a better chance of success because of the proliferation of point-of-sale-acceptance equipment and consumer ease with tap-and-go payments, says Randy Vanderhoof, director of the U.S. Payments Forum, an industry-advocacy organization based in Princeton Junction, N.J.

Given the experience in other countries, consumer adoption of NFC-based EMV cards may accelerate once consumers realize that tapping means not waiting for an audio cue to remove the chip card from the reader, Vanderhoof says.

While it may take a bit of time for consumers to catch on, Vanderhoof is optimistic. “We never had the levels of concentration of consumers being able to pay using the NFC or contactless interface before,” he says. “Clearly, the payment brands are very excited about this and more proactive in marketing their capabilities.”

Consistency, Please

And that could boost NFC even more in the U.S. payments market. “The dual-interface cards, both EMV chip and contactless, is expected to have an effect on the demand of new products and services, but issuing cards is not the greatest indicator,” says Krista Tedder director of payments at Pleasanton, Calif.-based Javelin Strategy & Research.

“Merchant acceptance of NFC needs to reach much higher levels before the demand is present,” she says. “For example, I purchased gas and was able to use NFC technology. At the same brand of gas station [a day later], I could not use the NFC payment because they only accepted swiped/dipped transactions at that gas station. Until there [are] consistent

experiences for the consumer, the consumer will revert to what they know works and will stop attempting to use NFC.”

Such inconsistency could bedevil greater NFC acceptance, especially because a consistent experience across all points of sale, along with supportive issuers and willing consumers,


form the three necessary components for payment acceptance to become widespread.

“We always see the chicken-and-egg scenario,” says Ammar Faheem, vice president of digital payments at Gemalto NV, a smart card maker and security-software provider. Having been posted internationally

Merrick Bank[®]

Merchant Acquiring

Portability • Profitability • Personalization



Partner with Us

MerrickBankAcquiring.com

Visit us at

<h4>MAC Level Up</h4> <p>Park MGM Las Vegas, NV March 11 - 14</p>	<h4>SEAA</h4> <p>Loews Atlanta Hotel Atlanta, GA March 25 - 27</p>
---	--



'We always see the chicken-and-egg scenario. When I was in Dubai, it was mostly contact-only EMV. Then Samsung Pay and Apple Pay came in and flipped how people buy.'

—AMMAR FAHEEM, VICE PRESIDENT OF DIGITAL PAYMENTS, GEMALTO NV

for Gemalto, Faheem has observed how different markets react when new NFC-based technology is introduced. Gemalto has headquarters in Amsterdam and France.

"When I was in Dubai, it was mostly contact-only EMV," Faheem says. "Then Samsung Pay and Apple Pay came in and flipped how people buy. Consumers there got used to tap-and-pay. That drove acceptance. Eventually, banks started issuing dual-interface cards. I saw the same in South Africa."

In the interim since the mid-2000s, mobile phones with tap-and-go capabilities using NFC chips have stepped in, relying on the same infrastructure as contactless cards. Apple Inc.'s Apple Pay, Google Pay from Alphabet Inc., and Samsung Pay from Samsung Electronics Co. Ltd., all have spent millions educating consumers about tap-and-pay. This may well aid contactless card adoption, some suggest.

"They've played an important role in shaping consumer behavior

in terms of payment habits," says Faheem. The Pays have also filled a "crucial role in marketing and promoting contactless technology as well as acceptance," he adds.

'Flipping a Switch'

While overall U.S. consumer adoption of mobile wallets is low—only 12% of all Apple Pay users are in the United States, says researcher Loup Ventures—adoption of contactless cards should be higher, says Vanderhoof.

What's Become of Host Card Emulation?

Host card emulation (HCE) is a technology that can be used to create an NFC wallet without using a chip, usually on mobile phones. Instead of storing payment credentials on a chip called the secure element, the data is managed in a cloud configuration controlled by the card issuer.

For a time, it was highly publicized and used in the United States, but lately it isn't as prominent as it once was. Google Pay is perhaps the best-known user of HCE technology in the United States. The technology is used more internationally, especially in developing markets where banks have more direct control of the mobile-payment experience.

"Host card emulation started to take off in 2014 and has provided significant benefits in mobile wallets," says Krista Tedder, director of payments at Javelin Strategy & Research. "HCE enables the mobile wallet to display the card on the device, including the logo of the bank/merchant to indicate which card it is. This provides consumers a comfort level that the product they are selecting is the one they want."

"For example," Tedder continues, "I have personal and business credit/debit cards, prepaid gift cards, and merchant-rewards programs loaded into my mobile wallet. I also have Walgreens prescription prepaid and airline QR codes. Knowing which product I am selecting makes the mobile wallet similar to a physical wallet."

Yet, the technology has some limitations.

"Every bank had a different kind of implementation," says Ammar Faheem, vice president of digital payments at Gemalto NV, a smart card maker and security software provider. "The other challenge with HCE is that it was limited to Android phones only."

Faheem says HCE-based wallets are still in use where the Pays have not yet launched, such as in many countries in Africa and the Middle East.

In the United States, the Pays are too far ahead for banks or other organizations to disavow NFC in favor of host card emulation. "It's about the user experience at the end of the day," Faheem says. "It's so much easier to click the button on my phone instead of going and finding a bank's application."



MAY 2019

SOMETHING BIG IS COMING

JOIN THE WATCHLIST AND STAY TUNED FOR THE ANNOUNCEMENT.

www.epicomingsoon.com



QR codes 'could work without any additional infrastructure, but on the other hand it must be implemented in some way on the merchant side.'

—KILIAN THALHAMMER, VICE PRESIDENT OF PRODUCT MANAGEMENT, PAYMENT, AND RISK, WIRECARD AG

The difference, and why there might be more NFC chips in use soon, is that the Pays generally only offer a payment function with limited rewards and offers, he says. Retailer mobile wallets often offer more.

"Mobile wallets without mobile offers will continue to struggle except in places where speed and convenience are of utmost concern," Vanderhoof says.

One card issuer, JPMorgan Chase & Co., may recognize this. In November, it launched Chase Offers, a rewards program for its credit and debit card holders.

Another factor that may aid NFC use is that the cost of chip cards has dropped since the U.S. market shifted to EMV in 2015. A non-printed, non-personalized contact-only EMV card may sell for less than 50 cents, Vanderhoof says. A dual-interface card may be approximately \$1, or less with volume orders.

"We were talking about multiples of \$2 and \$3 a card just a few years ago," he says, adding that there are

more than 1 billion EMV cards issued in the United States now.

QR codes, however, can be very inexpensive. Many companies provide QR-code generation online for free. Getting a code into a payments app, however, takes expensive developer time and integration into POS systems, especially if the mobile-payments program is captive to one retailer.

QR codes are not without a place in payments, as systems like Ali-pay have shown. "QR codes have a downside and an upside," says Kilian Thalhammer, vice president of product management, payment, and risk at Wirecard AG, a Munich-based payments provider. "It could work without any additional infrastructure, but on the other hand it must be implemented in some way on the merchant side."

That's not an issue with NFC. "With NFC built into the POS terminals, it's very similar to flipping a switch," says Aite's Peterson. "All of the processors have the capability to accept it. QR codes can require

a whole new layer of software to accept the payment. It's not a hardware change, but it's not an insignificant software change."

Lower Threshold

Will one win out over the other? Most observers contend there's room for both technologies in mobile payments, but it depends on the use case.

If offers are paramount and of enough perceived value to overcome any reluctance to use a QR code, that technology could be the choice. But if flexibility, ease of use, and advanced security are critical, then NFC may be the way to go.

"NFC capability requires merchants to rely on factors outside of their control," Tedder says. "The consumer must have an NFC device (either card or phone). This leaves out a large population of consumers who do not have access. With QR codes in mobile wallets hosted by merchants, the threshold of usage is much less—the consumer needs a mobile device which can take a picture." **DT**

'Mobile wallets without mobile offers will continue to struggle except in places where speed and convenience are of utmost concern.'

—RANDY VANDERHOOF, DIRECTOR, U.S. PAYMENTS FORUM



EVERYTHING YOU NEED

FROM ONE FAMILY OF COMPANIES



THE COMPANIES OF GENERAL CREDIT FORMS ARE READY TO MEET ALL YOUR POINT-OF-SALE NEEDS

Forms, Rolls & Labels ■ Custom Printing
POS Deployment, Depot & Configuration
Revenue Generating Supply Resale Programs
Custom Kitting, Distribution & Shipping
Purchasing & Inventory Management



www.gcfinc.com • 888.GCF.NEWS

FISERV'S BIG BITE



Executives at Fiserv Inc. all but popped champagne corks on Feb. 7 when they spoke to industry analysts about the Brookfield, Wis.-based company's financial results. It had been about three weeks since Fiserv stunned the payments business with its \$22-billion all-stock offer to buy First Data Corp., the big merchant and card-issuer processor, and its officials were finding the firm's banking clients in a welcoming mood.

Since the Jan. 16 announcement, said chief executive Jeff Yabuki, "We've spent a substantial majority of our time talking to clients, and [their] reactions have been incredibly positive." In fact, he told the analysts, "the feedback has been probably more positive than I would have thought."

The stock market also smiled on the deal. Between the day of the announcement and Feb. 13, Atlanta-based First Data's shares rose nearly 18% on the New York Stock Exchange, which overall climbed just less than 5%. Not a surprising result for the acquired entity. Fiserv's stock, though, shot up 16.2%, well outpacing the Nasdaq's 5.5% increase (chart, page 22)—a result that surprised some analysts who are accustomed to seeing companies' shares drop after announcing major deals.

The offer to buy First Data was a surprise on at least a couple of levels. First, the 43-year-old processor had shown few signs it was trolling for a buyer. Indeed, it has itself been a fairly aggressive acquirer since former JPMorgan Chase & Co. executive Frank Bisignano took over as CEO in 2013.

It has been especially keen to build up its fire power in point-of-sale technology (Clover, acquired in 2013), and in merchant sales and integrated payments (BluePay and CardConnect, respectively, snapped up for more than \$1.5 billion in 2017).

Second, while some may have mused about a deal for First Data, few people contacted for this story saw Fiserv as the probable buyer. The company enjoys a brisk business in core processing for financial institutions and also runs units involved in digital bill payment and person-to-person transactions. Two areas of overlap are services for bank card issuers and debit card networking, where First Data's Star network competes with Fiserv's smaller Accel system.

'Throwing off Cash'

What puzzles some observers is that the combination, after its expected close in the third quarter, will likely yield little in redundant products or services that could be cut or merged to help produce the savings the two parties are counting on. The companies project some \$900 million in combined revenue and cost savings annually by year five after the deal closes.

"There aren't obvious economies of scale because there's no overlap," argues Eric Grover, principal at Minden, Nev.-based financial-services consultancy Intrepid Ventures. "They can chop some overhead, but \$900 million in duplicative overhead, I don't think so."

Its \$22-billion megamerger agreement with First Data sets it up to be a dominant player on both the bank and merchant sides of payments. How will the industry react?

BY JOHN STEWART



Still, a deal of this size—almost certainly the biggest of its kind in the history of the U.S. payments business—doesn't pop out of a vacuum. In different ways, both companies saw advantages that were almost exclusively financial.

First Data would not comment for this story. Fiserv provided a four-paragraph statement lauding the services and technologies the combined entity will be able to deliver. "With this transaction, Fiserv will be better positioned to offer a broader suite of high-value client solutions with an even more extensive range of end-to-end capabilities," the statement says.

Certainly, Fiserv saw an opportunity to leverage the value of its stock, say some observers. "The EBITDA [earnings before interest, taxes, depreciation, and amortization] coming out of First Data is pretty steady," says Grover. "Even if those guys go off on a drunk, those businesses are still going to be throwing off cash."

But perhaps not quite enough cash. First Data's motivation isn't hard to see for those who've studied its balance sheet. One deal in recent memory that tops this latest one also involved First Data. It was Kohlberg Kravis Roberts & Co.'s \$29 billion leveraged buyout, which took the company private in 2007. That's about \$36 billion in today's dollars. First Data returned to public ownership in 2015, but KKR still controls about 41% of the equity.

More important, though it has been steadily paying down its debt from that deal, the processor is still saddled with an obligation of about \$17 billion. For some observers,

the Fiserv deal is mostly about that debt, which Fiserv plans to refinance.

"That didn't give [First Data] a lot of freedom to do things because of the covenants," says Peter Michaud, senior director of business intelligence at The Strawhecker Group, an Omaha-based payments consultancy. The covenants are the contracts put in place to control risk by restricting First Data's actions.

A public offering was a possibility, Michaud explains, but finding a partner was a more appealing option. "They really needed someone with a strong balance sheet and a lot of cash. Frank found the right partner," he says. So, perhaps, did private-equity giant KKR. It will hold approximately a 16% stake in the new company.

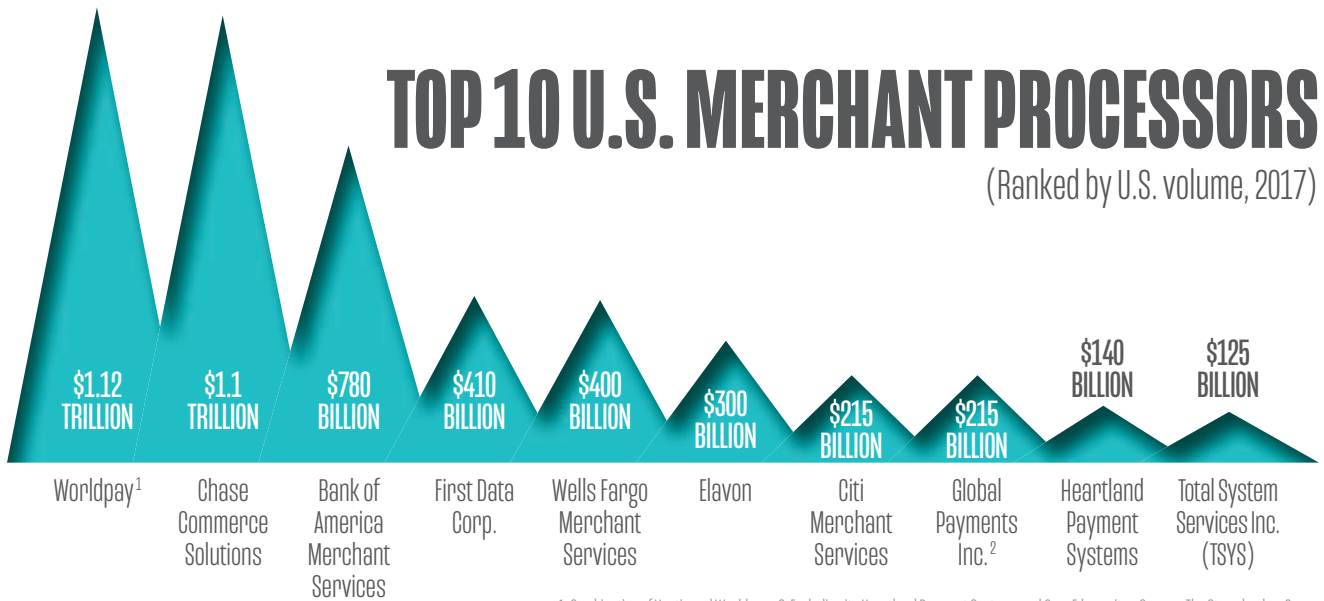
Playing Catch-Up

Now, as Michaud says, "innovation is going to be key" for the expanded Fiserv. Payments processing isn't the staid, back-office function it once was. Relatively recent entrants like Square Inc. and The Netherlands-based Adyen N.V. have grown fast and captured the industry's imagination with new twists on point-of-sale and gateway technology, respectively.

Investors have taken notice, and so have some of First Data's traditional competitors. Square has gone from trading in the low \$40s a year ago to the mid-\$70s in the middle of last month. Adyen went public late last spring at 438 euros per share (\$510 then) and closed at mid-month in February at 664 euros (\$750).

TOP 10 U.S. MERCHANT PROCESSORS

(Ranked by U.S. volume, 2017)



1. Combination of Vantiv and Worldpay. 2. Excluding its Heartland Payment Systems and OpenEdge units. Source: The Strawhecker Group

That's not even accounting for privately held Stripe Inc., which at its latest valuation is worth fully \$20 billion, up from \$9 billion. Stripe handles payments for e-commerce and gig-economy firms.

That leaves long-time processors playing catch-up, with some doing so more nimbly than others.

"What is really selling globally is technology-enhanced solutions," said Jeff Sloan, chief executive of Global Payments Inc., a First Data rival also based in Atlanta. He spoke last month to analysts covering his firm's earnings call.

Since 2012, Global has focused intently on buying and forging partnerships with business-software companies specializing in restaurants, health care, and other verticals, with the premise of infusing payments into their offerings.

With tech competition growing more fierce and engendering more value for processors, "getting additional scale makes sense for others that haven't been able to make those investments," Sloan said in response to an analyst's question about Global's take on the Fiserv-First Data deal.

But the big merger could have other impacts, as well. Some observers point to the access First Data may now

gain to the banking connections Fiserv has developed for core processing, peer-to-peer payments, and bill payment.

"The ability to have an extra set of tracks, going over banking rails, is pretty fascinating," notes Mike Mussaro, chief executive of Flywire Corp., a provider of cross-border payments. "No one is going in that direction. No one else is trying to put those things together."

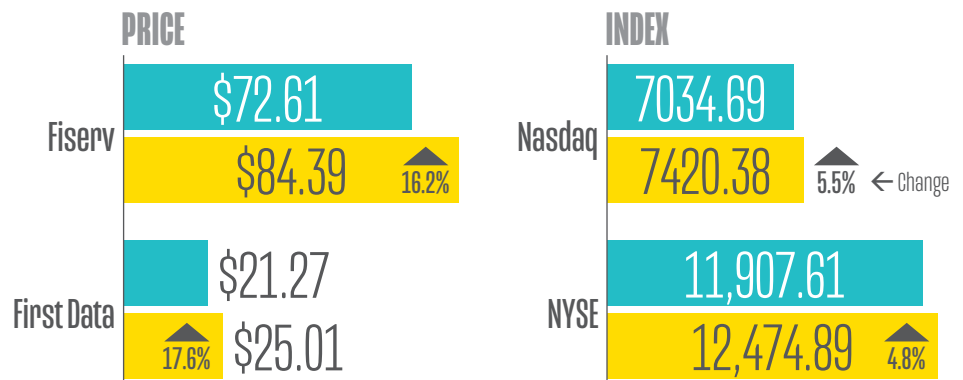
Filling a Gap

Others see potential here, as well. Fiserv runs its own P2P network, called Popmoney, but also connects it to Zelle, the national network created by some of the nation's biggest banks and operated by Early Warning Services, a bank-owned technology company. P2P payments have been among the first to benefit from banks' efforts to move money closer and closer to real-time speed.

"First Data has been quiet on faster payments, frankly, but they can benefit from what Fiserv has done to move the ball on that front," says Sarah Grotta, director of the debit and alternative products advisory service at Mercator Advisory Group, a Maynard, Mass.-based consultancy.

THE MARKETS SMILE ON THE DEAL

■ January 16, 2019
 ■ February 13, 2019



Note: Closing prices each day. Fiserv trades on the Nasdaq; First Data on the NYSE. Source: The markets

Next Is the New Now. **Your Possibilities Delivered.™**



Today's digital landscape exceeds the pace of change. That's why you need a strategy for what's next. And because next no longer means later, we've got a broad range of digital solutions and integrative technologies that will empower you to compete now. Join us.

Payments • Risk Management • Digital Banking • Analytics • Loyalty
Mobile • 24/7/365 Contact Center • Strategic Consulting



pscuc.com
844.367.7728

Likewise, that very thing Grover pointed to, a lack of overlap, could ultimately benefit Fiserv. This could start with the basic blocking and tackling of merchant acquiring, which has been a “gap” in Fiserv’s offering, says Patty Hewitt, a former Fiserv executive who is now an independent payments consultant and researcher and one of the few observers who wasn’t surprised to hear of the proposed merger. Through bank joint ventures and other channels, First Data is the biggest U.S. merchant processor.

Fiserv, she says, “looked in the past [at acquiring merchant processors], but the multiples were always too high. There’s only so much market left in core processing. It’s a declining market, highly mature. This is seen as their payments play. It’s been coming for a long time.”

One company many experts are focusing on now is Fidelity National Information Services Inc. (FIS), the sprawling Jacksonville, Fla.-based processor and banking-services provider seen as Fiserv’s closest rival.

Like Fiserv, FIS has had a hand in technology for real-time payments. “FIS has to take pause,” Hewitt says. “I think FIS has to react.” The logical reaction, she adds, would be to buy a merchant processor.

FIS refused to comment for this story, but CEO Gary Norcross let it be known in the company’s earnings call last month that his company is willing to open its wallet.

“We feel great about the position our company is in, about our ability to compete. That said, we would be interested in [potential deals],” Norcross said. “We want to find something that accelerates our growth rate. We think about wholesale banking and payments. There are a number of opportunities.”

‘That’s the Risk’

But not everyone is enthusiastic about the pending merger. Some see it as likely to suppress innovation rather than energize it.

Aaron Silva, founder of Paladin fs LLC, a firm that helps banks negotiate contracts with companies like Fiserv, fears vendor consolidation will only weaken banks’ position. “It may be good for Fiserv but it’s not good for the industry,” he says.

Rather than innovate internally, he argues, Fiserv and its competitors buy innovative companies and then raise the price of access to the newly acquired technology. “They’re holding on to cash to make acquisitions,” he says. “The fewer the suppliers, the worse it is for banks.”

On the merchant-processing side, Strawhecker’s Michaud has similar questions. For all the financial sense it makes, the deal may leave smaller ISOs in the cold, he warns, adding, “That’s the risk, servicing and customer service.” **DT**

A FIRST DATA TIMELINE

- 1971** Founded in Omaha to process for the Mid-America Bankcard Association
- 1976** Becomes first processor of bank-issued Visa and Mastercard cards
- 1980** American Express buys 80%, buys remaining 20% over next three years
- 1992** Goes public
- 1995** Acquires Western Union via acquisition of First Financial Management Corp.
- 1996** Forms First Data Merchant Services by combining Card Establishment Services and National Bancard Corp.
- 2004** Acquires Concord EFS
- 2006** Spins off Western Union as a publicly traded company
- 2007** Goes private via KKR leveraged buyout
- 2008** Dissolves joint venture with JPMorgan Chase in Chase Paymentech Solutions
- 2009** Partners with BofA to form Banc of America Merchant Services
- 2011** Collaborates with Google and other companies to launch Google Wallet
- 2013** Acquires Clover Network and Perka, a mobile-loyalty provider
- 2014** Becomes a token service provider with launch of Apple Pay
- 2015** Goes public again with largest U.S. IPO of the year
- 2017** Lays out \$750 million to enter ISV market with acquisition of CardConnect
- 2017** Pays \$760 million in cash for BluePay, a major ISO
- 2019** Agrees to be acquired by Fiserv Inc. in a \$22 billion all-stock transaction

Source: First Data



PAYMENTS FROM START TO FINTECH

APRIL 30-MAY 2, 2019 ►►► LAS VEGAS, NV

TRANSACT[®]
POWERED BY ETA

BE A PART OF PAYMENTS MOST POWERFUL NETWORK.

Join us to get the full picture of the power behind the payment. Network with executives of ISOs, VARs and ISVs, large financial institutions, networks, security and emerging technology companies, and start-ups looking to get into the payment space. Be a part of payments – from start to FinTech.

etatransact.com



So Many Irons in the Fire

Jim Daly

PayPal's octopus-like strategy covers everything from P2P payments, bill pay, and the point of sale to parting ways with eBay. Can Schulman and Co. keep all the balls in the air?

PayPal Holdings Inc. president and chief executive Dan Schulman can't be accused of making small plans.

"We aspire to be the de facto operating system for mobile and digital payments around the world, creating value for all of our partners and customers across the entire payments ecosystem," Schulman said Jan. 30 during PayPal's fourth-quarter 2018 conference call with analysts.

Action is backing up those words. Few financial companies have more going on at once than San Jose, Calif.-based PayPal. Just a few items on PayPal's to-do list include making its popular Venmo peer-to-peer payment service profitable, establishing a strong presence in bill payments after its acquisition of TIO Networks bombed, getting its halting effort to come to the point of sale into gear, successfully completing its separation from long-time parent company eBay Inc., and offering credit without getting burned.

What's the overarching strategy behind all this?

"They're trying to be relevant for the future," says Lawrence Berlin, a senior vice president at Chicago-based First Analysis Securities Corp.

who follows payment companies. "That's the key to everything."

Somewhat more ominous forces may be motivating PayPal, too.

"What we're seeing right now is a lot of evidence that PayPal realizes this is their game to lose," says Jordan McKee, research director of emerging payments technology at New York City-based 451 Research. "There's no shortage of threats."

Indeed, it seems everybody from fintech startups to established online processors such as Square Inc. and Stripe Inc. to big banks and Visa Inc. and Mastercard Inc., with whom PayPal has made peace recently, has some product or products that compete directly with PayPal. In the world of online and mobile payments, competitors can work with each other when their interests align, but interests can change rapidly.

Mobile Drives Growth

For now, however, PayPal holds a commanding position. Total payment volume (TPV) rose 27% year-over-year in 2018 to \$578 billion on nearly 10 billion transactions (chart, page 28). Net income for the year hit \$2 billion, up 15% from 2017's \$1.8 billion. Quarterly revenues surpassed \$4 billion

for the first time in the three months ended Dec. 31.

The worldwide active-account base expanded by about 38 million to 267 million, and some 21 million merchants now accept PayPal.

PayPal expects the good times to keep rolling. Chief financial officer John Rainey predicted on the January call that TPV will grow in the mid-20% range in 2019 and revenues will increase 16% to 17% on a currency-neutral basis.

And at a time when Apple Pay, Google Pay, and Samsung Pay are still struggling to win acceptance from consumers and merchants, PayPal racked up \$227 billion in mobile-payment volume in 2018, up 46% from \$155 billion in 2017, on 3.7 billion transactions.

"Mobile continues to drive our growth, with \$67 billion of mobile TPV in [the fourth quarter] alone, representing 41% of our total TPV," Schulman said.

Despite those achievements, PayPal's leadership believes much remains to be done to secure the company's position. One of its top priorities is generating revenue—and profit—from Venmo, PayPal's P2P payment service, which also features a social-networking platform. Venmo's volume jumped 79% in 2018 to \$62 billion, and Schulman expects volume to approach \$100 billion this year.

PayPal, which did not make an executive available to *Digital Transactions*



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

Today and every day follow

DIGITAL TRANSACTIONS

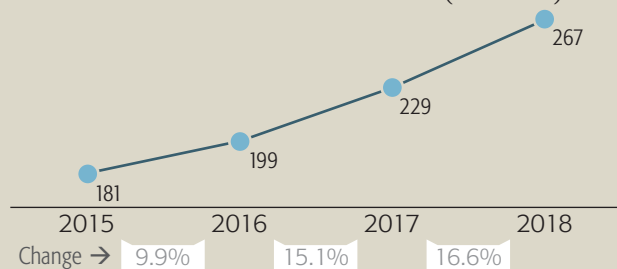
@DTPAYMENTNEWS on Twitter

DIGITAL
TRANSACTIONS

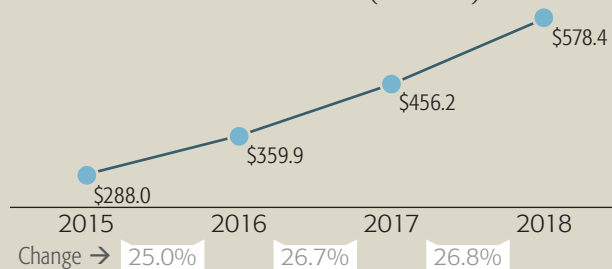
Trends in the Electronic Exchange of Value

Key PayPal Metrics

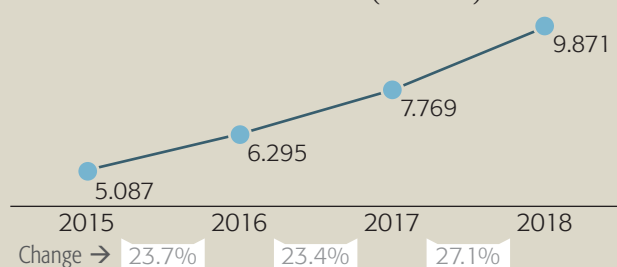
ACTIVE CUSTOMER ACCOUNTS (in millions)



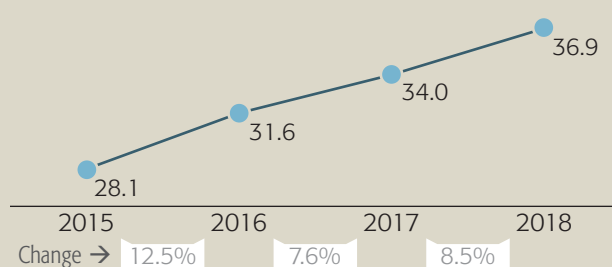
TOTAL PAYMENT VOLUME (in billions)



PAYMENT TRANSACTIONS (in billions)



PAYMENT TRANSACTIONS PER ACTIVE ACCOUNT



REVENUE AND INCOME (in billions)

	2015	Change	2016	Change	2017	Change	2018
Transaction revenues	\$8.22	16.6%	\$9.59	20.0%	\$11.50	19.2%	\$13.71
Other	\$1.03	21.9%	\$1.26	26.7%	\$1.59	9.4%	\$1.74
Total net revenues	\$9.25	17.2%	\$10.84	20.8%	\$13.09	18.0%	\$15.45
Net income	\$1.23	14.1%	\$1.40	28.1%	\$1.80	14.6%	\$2.06

Source: PayPal, Digital Transactions

to comment for this story, doesn't disclose the number of Venmo users. Payments researcher Richard Crone of San Carlos, Calif.-based Crone Consulting LLC estimates Venmo had 39 million active users at year-end 2018 versus 29 million for Zelle from bank-owned Early Warning Services LLC (chart, page 30).

Flywheel Effect

Venmo gains customers every time senders want to zap funds to non-Venmo users, who will need to open a Venmo account to access their money.

"They're growing their user base virally, all courtesy of the users,"

says Crone. "The flywheel effect is tremendous."

Zelle, however, has a larger average payment amount and is closing the gap due to rapid adoption from Early Warning's big-bank owners and from third-party processors offering it to smaller financial institutions.

But Venmo's biggest problem, like that of most P2P services, has been that consumers have proven highly resistant to paying fees to transfer money electronically. Providers are looking to monetize, in industry-speak, their systems by persuading merchants to accept them for payment of goods and services, and by charging fees

for value-added services such as real-time funds availability.

Venmo's Instant Transfer service, for example, enables users to get money out of their Venmo balance by transferring funds to an eligible debit card for a 1% fee, with a minimum fee of 25 cents and a \$10 maximum. Funds typically arrive within 30 minutes, compared with one to three days for standard transfers that go through the automated clearing house network.

Some 29% of Venmo account holders have made a "monetizable" transaction, producing a \$200 million revenue run-rate going into 2019,



Digital Transactions News

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

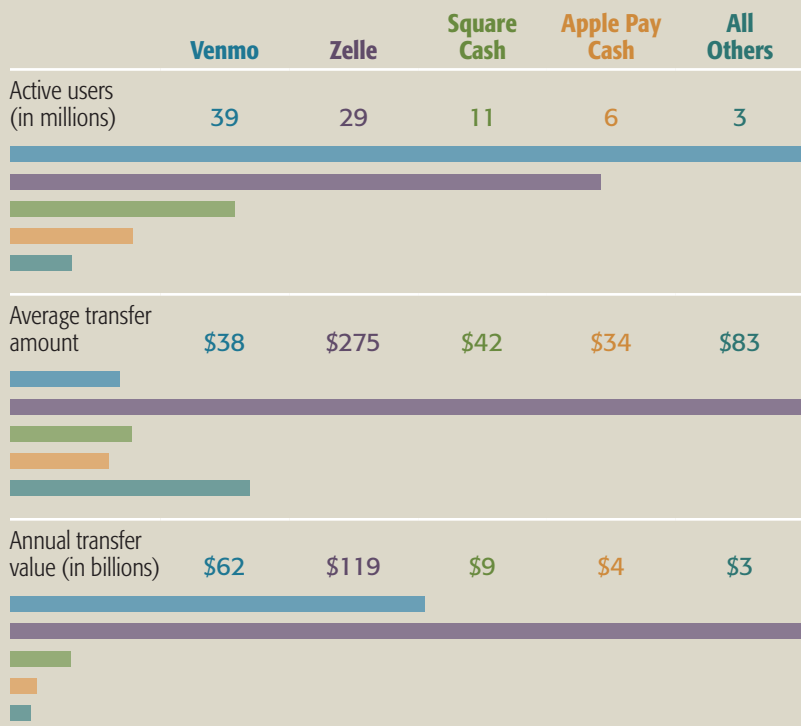
Digital Transactions News is packed with news and information from the \$123.4 billion transaction industry:

- ▶ 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.ameda.com/dtr/
or email publisher Bob Jenisch at Bob@digitaltransactions.net



The P2P Arena



Notes: Data as of 4q2018. Excludes \$77 billion in PayPal's non-Venmo P2P payments under the PayPal and Xoom brands. Active users defined as those making at least two transactions per month. Source: Company reports, Crone Consulting estimates

Schulman reported. A number of merchants, including Uber, the Grubhub food-ordering service, the movie and TV streaming service Hulu, and the Tidal music-streaming service, now accept Venmo for payments. About half the monetizable volume is coming from Instant Transfers, with the rest from payments on the Venmo Mastercard debit card and merchant sources.

Venmo's losses evidently were getting to be serious. Before the monetization effort kicked in in 2018, "we effectively were providing a service that we weren't monetizing in any way. And so the losses were growing as volume grew," Rainey said. He added that the immediate goal is to break even, a target PayPal probably won't hit within two quarters.

Another big market PayPal is eyeing is bill payments, a niche where it made a rare misstep. PayPal thought its \$238 million acquisition of

Vancouver, British Columbia-based TIO Networks in 2017 would help it establish a major presence in electronic bill-pay thanks to TIO's connections with 10,000 billers through a network of 900 kiosks, 65,000 walk-in locations, and 14 million consumer accounts doing \$7 billion in annual volume.

But before the year was out, a data breach that potentially affected 1.6 million customers forced PayPal to suspend the network's operations. Last March, PayPal said it would shut TIO down.

Now PayPal is trying again by forming a partnership with Paymentus Corp. The company didn't disclose details of its agreement with the Charlotte, N.C.-based processor, but on the January call PayPal chief operating officer Bill Ready said the partnership potentially could generate "tens of billions" of dollars in bill-payment volume. Paymentus's Web site says

the firm was founded in 2004 and has 1,300 clients, including "some of the largest billers in North America."

A Bet That Didn't Work Out

PayPal's top brass clearly hopes Paymentus will help the company recover its bill-pay mojo. Surprisingly, PayPal received little public thrashing from Wall Street over the TIO flame-out.

"They were not really punished because it was small," analyst Berlin says, noting that the \$238 million PayPal plunked down for TIO Networks was tiny compared with its revenues and market capitalization.

Adds McKee of 451 Research: "Not all bets are going to work out. Some might end up like TIO Networks, and some might work out like Braintree." The latter, of course, is the highly successful online-commerce processor and Venmo owner, headed by Ready, that eBay bought in 2013 for \$800 million and put under PayPal's wing.

Another problematic area PayPal continues to work on is bringing its service to the point of sale. The company has deployed various strategies. At one time or another, it has worked with partners, including Discover Financial Services, in pursuit of this elusive goal, so far with little to show for its efforts.

"The one thing they haven't figured out is the physical world," says Thad Peterson, senior analyst and e-commerce researcher at Aite Group LLC, Boston. "As near as I can tell, they still don't have a clear strategy on what they want to do, or if they have, they haven't revealed it yet." But he adds: "It's probably the latter, not the former."

At times, however, parts of the strategy reveal themselves. In its biggest acquisition ever, PayPal last September bought Stockholm-based payments firm iZettle AB for \$2.2 billion. Founded in 2010, iZettle often is called the "Square of Europe" for the similarities of its business model with

that of San Francisco-based Square, which started out by providing tiny businesses and part-time sellers with a dongle for smart phones so they could accept credit and debit cards.

iZettle targeted small and mid-size businesses with its mini chip card reader and has branched into other payments niches, including POS software, e-commerce, and contactless payments.

Today iZettle serves about 500,000 merchants in 11 European and Latin American countries. The acquisition doesn't do much for PayPal's POS expansion in its home country, but it does advance yet another company goal, that of being a major international payments player.

'Common Thread'

PayPal took a further step in that direction last year when it bought San Francisco-based payout provider Hyperwallet for \$400 million in cash. Hyperwallet is an international specialist in provisioning payments, commissions, and royalties to drivers, recording artists, and other groups of independent workers.

The iZettle and Hyperwallet acquisitions show PayPal is "trying to move ... offline and international, that's the common thread," says Berlin.

In some ways, PayPal finds itself haunted by its own history. It is in the final stages of separating from eBay, which owned it for 13 years but spun it off in 2015. Under a five-year operating agreement, PayPal has remained the online marketplace's payments provider.

But that picture started getting murky last year. In September, eBay said it has "begun managing payments" on its massive marketplace and that it expects to have a majority of sellers converted to the new program by 2021. Earlier in the year, eBay contracted with Adyen, a Netherlands-based gateway with U.S. operations based in San Francisco, to relay transactions to a wide range of payment methods and relegated

PayPal to the role of just one of those payment choices.

eBay in January revealed that some 3,500 sellers had migrated to its new payments platform by year's end at an average 25% discount to PayPal's published transaction fees.

PayPal's top brass says all of the company's non-eBay businesses are filling the eBay void. Schulman noted on the recent call that eBay generated "zero growth" for PayPal in the fourth quarter and that it accounted for only 10% of TPV, down from 13% a year earlier.



'We aspire to be the de facto operating system for mobile and digital payments around the world.'

—DAN SCHULMAN, PRESIDENT AND CHIEF EXECUTIVE, PAYPAL HOLDINGS INC.

"We're able to absorb that because of the breadth of our portfolio," he said, adding that "eBay is going to be a much smaller part of our business than any of us thought it would be" by 2020, when the operating agreement officially expires.

"The message that I got out of that was, 'we're not dependent on them in any way whatsoever any more, we've got so much going on,'" says Aite's Peterson.

Exiting the 'Risk Business'

PayPal has shown in other ways that it will step back from a business it's in, even if it doesn't exit it entirely. The company, which offers the PayPal Credit service to consumers and PayPal Working Capital to merchants, recently noted that it has lent \$50 billion to American consumers since eBay acquired the BillMeLater lending service 11 years ago, and, as with Braintree, put it under PayPal's wing.

While fintechs like PayPal and its competitors want to give consumers and merchants access to credit, PayPal has concluded it doesn't want the exposure of being a lender. Last July,

it sold its U.S. consumer credit portfolio to Synchrony Financial for about \$6.5 billion in cash.

"That tells me they want to be out of the risk business," says Peterson. "Given the potential for a downturn in the economy, I think it was the right move."

But as its longstanding relationship with eBay sunsets and it treads carefully with credit, PayPal is elevating so-called "partnerships" with online marketplaces, merchants, networks, banks, and others into the top tier of its growth strategy. The company

has struck no fewer than 38 "strategic agreements" since 2016 with everyone from Visa, Mastercard, American Express, and Discover to Facebook and more recently Walmart Inc., according to a recent investor presentation. Under a service launched in November, PayPal account holders can go to 4,700 Walmart locations to load or withdraw money from their PayPal accounts.

PayPal's accords with Visa and Mastercard essentially called for PayPal to encourage account holders to use more card-based funding for their accounts in contrast to PayPal's traditional preference for funding through the low-cost ACH. The change put some pressure on PayPal's transaction margins but resolved what appeared to be a growing conflict with the card networks.

"I don't think you want to go to war with Visa and Mastercard," McKee says.

McKee notes that many observers had doubts about PayPal when eBay spun off it off. Those doubts are largely settled. "Right now, they've kind of proven that they're able to stand on their own," he says. **DT**



PCI's Latest Security Gambit

Taylor Armerding

New software standards aim to resolve—or at least minimize—credit card theft. There's cause for both optimism and caution.

Probably you've seen the headline, or a version of it, multiple times: "Another day, another data breach." As in, cyber insecurity is rampant.

It is especially rampant when it comes to the theft of credit card data. At least one estimate, from threat-intelligence firm Gemini Advisory, puts it at 60 million stolen cards just from U.S. owners during a 12-month period ending last Nov. 1 (chart, page 33). Do the math. That's an average of another day, another 164,384 card numbers stolen.

Which means anything that might reverse, or even slow, that trend would be revolutionary, in a very good way. And that is the aim of the Payment Card Industry Security Standards Council (PCI SSC). In mid-January, it published the first major, global overhaul of its software-security standards in more than a decade.

The titles of the new standards are a scramble of acronyms. The PCI Secure Software Standard (PCI SSS) and the PCI Secure Software Lifecycle (PCI Secure SLC) Standard are part of a new PCI Software Security Framework (PCI SSF) that will eventually replace the PCI Payment Application Data Security Standard (PA-DSS), created in 2008 but updated several times since then, most recently in 2016. You might need a reference card to keep track of all that.

And while the council clearly aspires to change things for the better, it acknowledges up front that they won't change quickly—not next week, next month, perhaps not even until next year. The PA-DSS will not be "retired" until 2022.

Will Reality Match Intent?

Still, Matthew Getzelman, principal consultant at Synopsys Inc., calls the new standards "transformational—a whole new expectation for developing and maintaining secure software."

"The PA-DSS is applicable to direct payment applications only—apps that directly process credit cards. The new standards apply to all application development in the PCI DSS space," he says.

Or as Troy Leach, PCI SSC chief technology officer, put it, the new standards address the evolution of software development "with an alternative approach for assessing software security ... designed to help ensure payment software adequately protects the integrity and confidentiality of payment transactions and data."

The key principles are:

- ▶ Critical asset identification
- ▶ Secure default configuration
- ▶ Sensitive data protection
- ▶ Authentication and access control
- ▶ Attack detection
- ▶ Vendor security guidance

The intent is "to demonstrate the ongoing protection of payment data by the software that stores, processes, or transmits that information," Leach said.

That is a lofty, and worthy, goal. How realistic is it?

Sammy Migues, chief scientist at Synopsys, served on a working group for several years that had a hand in developing the standards. The "intent and philosophy" of the new standards are transformational, he says, but it will take some time to see if the reality matches the intent.

Even so, he says he is encouraged that the language spelling out requirements for security testing is more precise and detailed.

'Reasonable Code'

Instead of simply requiring penetration testing and static application security testing (SAST), the new framework calls for a variety of specific security-testing tools and techniques.

"At a minimum, assessors must use the appropriate combination of static and dynamic analyses to validate each control objective," the framework says, citing tools for "automated static analysis security testing (SAST), dynamic analysis security testing (DAST), interactive application security testing (IAST), and software composition analysis (SCA) tools—as well as manual techniques such as manual code reviews and penetration testing."

Migues said this is likely to ensure that “some vendors are not just luckily passing some pen tests, but are consistently writing reasonable code.”

Nonetheless, he sees the changes as more incremental than revolutionary. “It took 10 years to make a small change in direction and intent, and it’ll take three-plus years to make it stick,” he said.

But whatever the magnitude of the changes, the long-term results will also depend in part on how much of the industry complies with them and whether online attackers figure out new ways around improved security, as they always do.

In the past, compliance has been spotty among smaller organizations. They argue they don’t have the resources and expertise to comply, even though failure to comply can put them on the hook for sanctions, fines, and liability if they are breached. But Leach said the new standards are intended not for merchants but for their software providers.

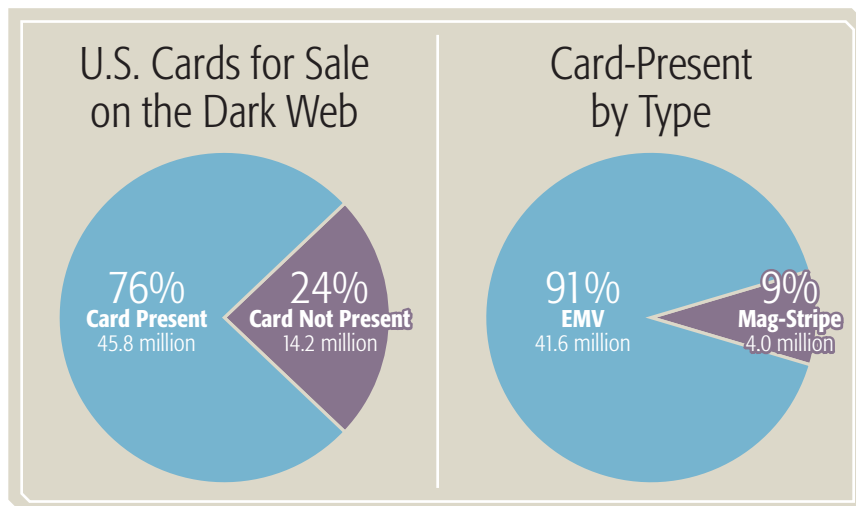
“This probably benefits [small-to-medium-size businesses] more than any other group,” he said. “It provides independent security testing of software to allow companies to make a more informed decision prior to purchase.

“Businesses that may not have the internal resources or capabilities to test the security of software they use to accept payments can use the standard as a metric to know their customers will be protected,” he said.

Still, while the intent and motive of the new framework are obviously laudable, Migues remains skeptical about the impact it will have.

“There is no objective evidence to indicate that the PCI standards have resulted in material improvements that wouldn’t have resulted through natural marketplace evolution and vendor attrition,” he says.

“Given that PCI compliance requires just a minimum level of application/system security, there was and still is no economic incentive to



Note: Data for October 2017 to October 2018.

Source: Gemini Advisory

be better than that. I’m not aware of any data that suggest PCI-compliant systems are penetrated any less often than any other systems.”

Hope Or Reality?

Leach acknowledged that the PCI SSC doesn’t have such evidence, but said there are “several sources in the industry that have such evidence, but it is something we are not privy to.”

And he said the council has heard anecdotally “from several companies over the years that have benefited by

using software that was independently tested by security experts that prevented potential exploits.”

There’s no debate that better software security will improve the security of the payment card industry overall. But will it cut the daily average of card data stolen to something less than 164,384? That is the hope, but it’s much too early to know if it will be the reality. **DT**

Taylor Armerding is senior infosec writer at Synopsys Inc., Mountain View, Calif.

The advertisement features the USAePAY logo at the top left, with social media icons and the handle @USAePAY to the right. Below the logo is the tagline "SMARTER SOLUTIONS FOR SECURE PAYMENTS". The ad is divided into three sections: "Retail" showing a payment terminal, "Ecommerce" showing a laptop with a dashboard, and "Mobile" showing a smartphone and tablet. At the bottom, the phone number 866.490.0042 and the website USAePay.com are displayed.



Cryptocurrency's Weakest Links

Peter Lucas

To purloin crypto, hackers are importing successful—and very familiar—methods from the world of fiat money. Here's what experts say needs to be done.

Security has always been a big selling point for Bitcoin and other cryptocurrencies. The crux of the security argument is twofold. Unlike cash, cryptocurrencies are encrypted in a digital wallet that can only be unlocked with a private key so mathematically complex that it's considered hacker-proof.

Plus, every cryptocurrency transaction is recorded in the blockchain, an up-to-the-minute ledger that requires verification for each transaction from multiple parties.

This double layer of security, cryptocurrency evangelists say, makes cryptocurrency incorruptible and as fraud-resistant as money gets.

In theory, cryptocurrency security is tighter than that of Fort Knox. But theory is not always reality. Criminals, as they so often do, find weaknesses in crypto defenses. Instead of directly attacking the blockchain or the cryptography that protects private keys, fraudsters are relying on the same social-engineering techniques they use to hack the databases of financial institutions and corporations.

These techniques include phishing and malware attacks that target employees of cryptocurrency exchanges or individual users. These attacks often occur via email.

Domain-name system (DNS) hijacking is another familiar scam. This ploy exploits weaknesses in the DNS so a criminal can replace a legitimate Web-site address with a phony address that redirects the exchange's traffic to a phony Web site that looks just like the exchange site but is controlled by the criminal. When cryptocurrency users enter their private key on the phony site, the data goes straight to the criminal.

Social-engineering scams are intended to produce the same result: Trick cryptocurrency users into unwittingly giving up their private keys. Once in possession of the private key, criminals can empty a cryptocurrency user's wallet.

Since cryptocurrency is uninsured by a government, unlike cash deposits held in U.S. banks, for example, crypto users have no way to recoup all, or part, of their losses due to theft.

Compounding the problem is that cryptocurrency ensures anonymity. While the blockchain requires multiple parties to validate a transaction, it does not provide a record of who actually makes a transaction.

That means criminals who trick an unwitting consumer to hand over his key won't leave a paper trail after absconding with the victim's funds.

That's because all the keepers of the blockchain see is that the private key was used to unlock the wallet.

Bottom line, cybercriminals are simply importing tried-and-true methods from the world of fiat money.

"Cryptocurrency hackings today have nothing to do with the math behind the private keys, the issues are with the security around protecting the keys themselves," says Ahmet Tuncay, chief executive of Sepior, an Aarhus, Denmark-based provider of security solutions for cryptocurrency and blockchain applications.

Eye-Popping Losses

Cryptocurrency's vulnerability to social engineering has produced some eye-popping losses. In 2018, cyberthieves made off with \$1.7 billion in cryptocurrency, according to Menlo, Calif. Park-based CipherTrace Inc., a provider of cryptocurrency and blockchain security solutions.

Criminals have kept up their torrid pace in 2019, pocketing \$150 million in cryptocurrency in January alone, and show no signs of slowing down, even though the prices of cryptocurrency have dropped, CipherTrace says.

Of the losses incurred in 2018, \$950 million was heisted from cryptocurrency exchanges that allow consumers to buy, sell, and store digital currencies. That amount was three times more than what was stolen from exchanges in 2017, CipherTrace says.

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

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 takeouts.

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

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

The huge jump in losses incurred by exchanges is an indication that with each successful theft, criminals become emboldened to pull off bigger heists, security experts say.

That makes exchanges prime targets, as they house the largest caches of cryptocurrency. Indeed, two Japanese exchanges were hit for \$600 million in combined losses in 2018, according to CipherTrace. The first heist, which occurred in January 2018 against the Coincheck exchange, totaled \$530 million and affected a reported 260,000 investors.

That amount shattered the previous record of \$400 million in Bitcoin stolen from Mt. Gox in 2014. Nine months later, cryptocurrency firm Tech Bureau Corp.'s exchange was hit for \$70 million in losses by cyberthieves.

The balance of crypto thefts occur in one of two ways. One way is for criminals gain access to consumer wallets stored outside an exchange. For example, they might take over a consumer's Internet-enabled device to steal his private key.

Or they might deploy cons in which investors are approached to use cryptocurrency to purchase shares in a new exchange or company developing new blockchain technology, only to see criminals vanish with their funds. The scam is often referred to as an initial coin offering, since in an ICO cryptocurrency is the funding mechanism for raising investment capital.



Source: CipherTrace

Smaller-scale scams include creating fake sites that purportedly sell secure cryptocurrency wallets to consumers wishing to manage their wallets on their own. More often than not, these wallets appear to be legitimate, but have been compromised and are being resold. Consequently, any money deposited into the wallet is rerouted to the criminal marketing the wallet.

“If a consumer wants to manage [his] own keys in a cryptocurrency wallet, he needs to be certain he is buying the wallet direct from the manufacturer,” says David Jevans, chief executive of CipherTrace. “Criminals

targeting cryptocurrency usually have degrees in technology and understand the world cryptocurrency trades in, so they’ve developed a lot of ways to get people to part with their private keys.”

That insight is why criminals targeting cryptocurrency have about a six-month lead on market security practices, Jevans says.

Wallets Hot And Cold

Closing the gap will require exchanges and consumers to recognize the need for better security hygiene. “Exchanges are getting hacked for the same reasons banks, credit bureaus, and companies do—failure to properly enforce security practices,” says Gideon Samid, chief technology officer for McLean, Va.-based BitMint, a digital currency. Samid also is this magazine’s security columnist (page 12).

Best practices start with educating employees of exchanges about the risk of opening emails from someone other than a trusted sender. Criminals can disguise phishing emails with legitimate corporate logos or email addresses similar to a trusted sender.

“There are emails that can be made to look like a memo to all



employees from the CEO,” says Kim Grauer, a senior economist for Chainalysis Inc., a New York City-based provider of blockchain security and compliance applications.

Opening a suspicious email can launch malware into the system that captures passwords and other vital data needed for unlocking wallets. “That’s why employees need to be trained that if they click on a suspicious email or link, they need to report it immediately,” Grauer says.

Vigilance against phishing attacks, however, is not enough to keep hackers completely out, as a few are bound to slip through this line of defense. That’s why storing cryptocurrency in a cold wallet can be an effective solution for preventing losses.

Unlike hot wallets, which are continuously connected to the Internet to allow around-the-clock access to

‘Exchanges should be breaking up storage of cryptocurrency between hot and cold wallets.’

funds stored in them, cold wallets store cryptocurrency offline, making them immune to an attack via an Internet connection.

Keeping the majority of cryptocurrency holdings in cold wallets can prevent huge losses. “Exchanges should be breaking up storage of cryptocurrency between hot and cold wallets,” Jevans says. “If an exchange has \$500 million in cryptocurrency, it may really only need \$30 to \$40 million live at any one time.”

Keeping cold wallets on servers that have never been connected to the Internet and transferring the funds to a

hot wallet via a single use flash drive can provide an even stronger layer of security.

To move funds in this environment, which is sometimes referred to as deep cold storage, funds are downloaded to a flash drive that has never been connected to an Internet-enabled device. Wallets in cold storage are opened by entering the private key.

After the funds are downloaded, the flash drive is connected to a server containing the hot wallet into which the funds are transferred. The flash drive is then destroyed or disposed of



DigitalTransactions.net

brings you the most important payments market news, in one place, updated the moment it happens

Breaking news from the payments market, posted daily	Concise, clean interface is easy to navigate	Calendar of industry events
Complete current and past issues of <i>Digital Transactions</i> magazine	Detailed listings of payments market suppliers	13 years of payments news and analysis

DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

as a precaution against any contamination from malware.

“Consumers managing their own wallet can benefit from cold-wallet storage too,” Jevans says. “It requires an [offline] computer dedicated to managing the account.”

‘Step Up And Lead’

Security experts also recommend cryptocurrency users never store their private keys on a computer connected to the Internet, a smart phone, or in an email sent to themselves.

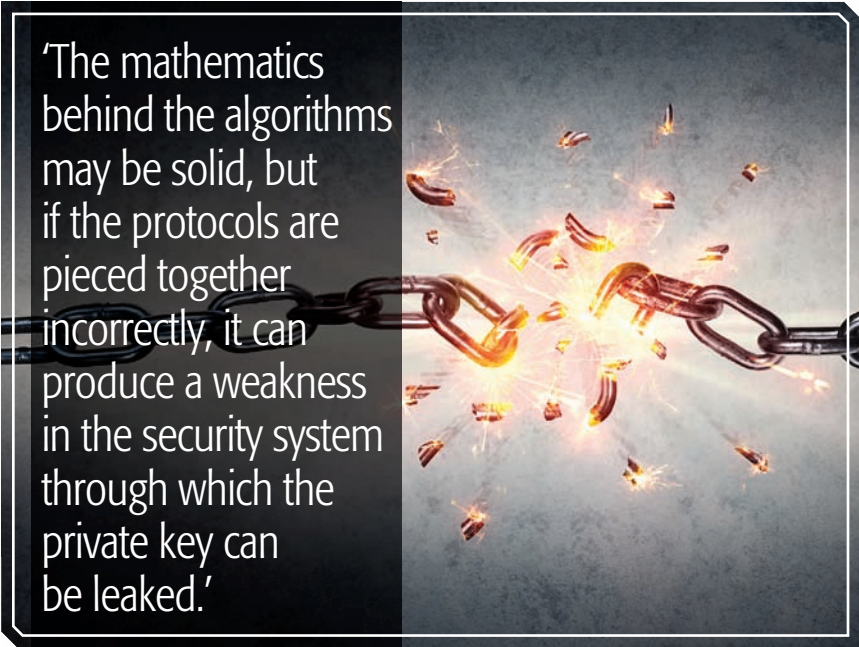
“Write the code out on paper and put it in a safe place,” Jevans says. “If a consumer elects to have an exchange store their wallet, be sure to perform due diligence on the exchanges’ security measures and make use of all the security tools it provides.”

Consumers and exchanges should also be sure to keep their anti-virus and anti-malware software up to date.

Performing due diligence on an exchange that offers wallet-management service is critical, because many of them are startups with little or no track record when it comes to security. And like many businesses, exchanges also must contend with a shortage of skilled security technicians, says Rick McElroy, head of security at Carbon Black Inc., a Waltham, Mass.-based cybersecurity company.

“A lot of new exchanges are more focused on getting up and running first, as opposed to security,” McElroy says. “Someone has to step up and lead on cryptocurrency-security management, and exchanges can be the ones to spark the charge.”

One step exchanges can take to lead the charge on security is requiring multiple signatures on the transaction record to verify and record the transaction approval. Many cryptocurrencies, including Bitcoin, record either a single signature or a composite of multiple signatures, because this is a simple, low-cost solution to implement. Single signatures are only secure, however, if the single private key is secure.



‘The mathematics behind the algorithms may be solid, but if the protocols are pieced together incorrectly, it can produce a weakness in the security system through which the private key can be leaked.’

A more secure signature-authentication method is to require multiple different parties to approve a transaction. This option is quite costly and can raise transaction fees, which means it has limited implementation, says Sepior’s Tuncay.

An alternative to multi-signature technology is ThresholdSig, which allows multiple different parties to collectively approve a transaction, but record it on the blockchain as a single signature.

“Rather than generating entire keys, ThresholdSig uses a technique called Multiparty Computation to generate shares of a single key on the device used by each approver,” Tuncay says. “An entire key is never produced or stored on any device at any time. These attributes dramatically reduce the potential for key theft and cost less to implement, which holds down transaction costs.”

Weaknesses

Not all thefts are the result of email tricks and other established tactics. Above all, cryptocurrency users need to guard against overconfidence about the strength of the cryptography used to secure private keys. While there are no known incidents

of criminals cracking these codes, some cryptography experts argue it can be done.

One potential weakness lies in the assembly of cryptographic protocols. “The mathematics behind the algorithms may be solid, but if the protocols are pieced together incorrectly, it can produce a weakness in the security system through which the private key can be leaked,” says Nicko van Someren, chief security officer for Nanopay, a Toronto-based payment platform for real-time multi-currency payment solutions.

History has also shown that any mathematical equation can be solved either by a smarter mathematician, someone with the computing power to crack the code, or both. “Few people delve into the math behind cryptography to determine how strong it really is,” says Samid. “I’ve seen predictions that the cryptography behind Bitcoin will be cracked in 10 years.”

It’s an ominous prediction that, if proven true, could rock the cryptocurrency world to its core. “Security is something that a lot of crypto users don’t want to learn or think about, but it’s not a given,” Samid says. “There are a lot of threats and they can’t be ignored.” **DT**

No brand is future-proof, but PayPal's commitment to pragmatism, inspiration, and innovation makes it very hard for competitors to dethrone.

PayPal: Secrets of a Relentlessly Relevant Juggernaut

Staying on top in payments requires close attention to a few ironclad rules, say Saurabh Wahi and Davis Ward.

In the fourth annual Prophet Brand Relevance Index (BRI), PayPal Holdings Inc. was once again, and by far, the best-performing financial-services brand. It's not just that it continues to outperform such competitors as Visa Inc., American Express Co., and Mastercard Inc. In one key measure—trustworthiness—it even beats digital powerhouses like Amazon.com Inc., Apple Inc., and Alphabet Inc.'s Google.

Although it celebrated its 20th anniversary last year, PayPal manages to feel and behave like a startup. Even as it continually causes disruption through innovation, acquisition, and unexpected partnerships, it fends off constant threats. Yet, it never seems to take its eye off improving core products and services.

How does a brand build such endurance? To find out, we dug deeper into each component of relevance. While PayPal performs well on all four drivers of our Index (customer obsession, ruthless pragmatism, distinctively inspired, pervasively innovative), it soars in three.

First, it ranks fourth among all brands in ruthless pragmatism, where it beats names like Netflix, Android, and Samsung. Second, it scores very highly on certain distinctively inspired attributes. Finally, PayPal excels across certain pervasively innovative measures. A closer look at those numbers reveals three lessons PayPal

can teach all brands about becoming more relevant to their customers:

Create ever-improving experiences

Ruthless pragmatism is all about delivering the experiences that consumers expect—when, where, and how they need them. PayPal eclipses almost every other financial-services brand on the important attributes of “makes my life easier,” “delivers a consistent experience,” and “I know I can depend on.”

That's because PayPal knows that what matters most to people is the experience of each interaction. Are transactions fast? Hiccup-free? Intuitive, whether it's a one-and-done mobile purchase or an elaborate desktop order?

The company constantly redefines its digital experiences, with the latest version of its app making it even more seamless to send and receive funds. It recently introduced “smart buttons” as checkout options for merchants. Using artificial intelligence (AI) to detect what type of payment you are likely to use, it cuts down on Web-site clutter. This is a seemingly invisible change to consumers, yet makes for a quick and pleasant experience.

As a result of these investments, consumers see PayPal as a brand that is devoted to helping



Saurabh Wahi (top) is a partner, and Davis Ward an associate partner, at Prophet, New York City.

them manage their daily financial lives. That's why it also scores so highly on "meets an important need in my life."

Inspire your audience

A key to being distinctively inspired is earning the trust of consumers. Of the thousands of brands we measure, PayPal ranks fifth in trustworthiness. Not only is PayPal far ahead of other payment methods (only Visa, at No. 42, even makes the top 50) and financial brands, it's seen as more trustworthy than Amazon (No. 6), and is far ahead of Apple (No. 33) and Google (No. 117).

In an environment where data security is top of mind, PayPal's history of working hard to build trust with its consumers is paying off. Within our smart and connected landscape, the wallet is sacred when it comes to trust. When people see the PayPal button on a Web site, they breathe easier when they buy.

It also does a better job of conveying its commitment to safeguard users. These measures include the recently-advanced authentication features, 24/7 fraud monitoring, and instant account notifications.

Another way that companies inspire people is through brand purpose. PayPal rates higher in "has a purpose I believe in" than any other financial brand. This metric could reflect the company's growing efforts to become a social engine of change through programs like LoanBuilder and PayPal Working Capital.

And its new deal with Walmart Inc., allowing customers to deposit and withdraw cash for a small fee in stores, is perhaps its biggest commitment yet to helping the millions of Americans who earn too little to have a bank account.

Make innovation an everyday obsession

In its quest for pervasive innovation, PayPal seems to be pursuing newness in three areas. First, it's concentrating on organic and internal inventions,

including the increasing use of AI and early forays into blockchain.

Next, it uses acquisitions to broaden and modernize its offerings. Besides owning Venmo, which infuses PayPal with vast amounts of data about how Millennials use payment services, it recently bought: iZettle AB, a \$2.2 billion deal that expands the tools and platforms it can offer small businesses; Jetlore Inc., an AI startup focused on personalizing commerce experiences that can predict what color, size, and styles customers choose; and Hyperwallet Systems Inc., a \$400 million deal for a company that distributes payments to merchants in multiple currencies. And, earlier, it added Xoom Corp., which lets people transfer money and pay international bills easily.

Finally, PayPal expands its ecosystem through key strategic partnerships.

It thrives by bringing other companies, sometimes even competitors, into its tent, including Apple, Samsung Electronics Co. Ltd., Facebook Inc., Google, Visa, and Mastercard, as well as banks like JPMorgan Chase & Co. and Bank of America Corp.

Of course, no brand is future-proof. There's no guarantee that PayPal's two decades of success can safeguard it from what's ahead. For example, Zelle, the payments platform launched by a consortium of 30 large banks, is coming hard for Venmo, and leading forecaster eMarketer expects it to barrel past Venmo this year.

But what's clear is that PayPal's commitment to pragmatism, inspiration, and innovation makes it continually more relevant and meaningful to consumers, and very hard for competitors to dethrone. **DT**

ADVERTISER INDEX

Cutter Financial 610-451-4096	Page 7 www.cutterfinancial.com
Digital Transactions 877-658-0418	Pages 27, 29, 35, 37 www.digitaltransactions.net
Electronic Merchant Systems 866-887-8907	Inside Back Cover www.emsagent.com
Electronic Payments 800-966-5520	Page 17 www.epicomingsoon.com
eProcessing Network 800-296-4810	Page 11 www.eprocessingnetwork.com
EVO 855-795-0635	Page 13 www.evopayments.cc/simplify
First American 866-464-3277	Page 9 www.first-american.net/iso-partnerships
General Credit Forms 888-GCF-NEWS	Page 19 www.gcfinc.com
Harbortouch 800-201-0461	Page 1 www.harbortouchroadshow.com
Humboldt Merchant Services 855-767-0685	Back cover www.hbms.com
iStream Financial Services 262-796-0925	Page 5 www.istreamfs.com
Magtek 562-546-6467	Page 3 www.magtek.com
Merrick Bank 800-267-2256	Page 15 www.merrickbankacquiring.com
PAX 877-859-0099	Inside Front Cover www.pax.us
PSCU 844-367-7728	Page 23 www.pscu.com
Transact Powered by ETA	Page 25 www.etatransact.com

No Good Merchant Left Behind.



CNP Specialists



Retail Experts



Industry Leading Portfolio
Management Tools



Latest Next Day Funding
Window in the Industry

Learn More

Call 866.887.8907
Visit [emsagent.com](https://www.emsagent.com)



AGENT





Where growing your portfolio comes naturally.

At Humboldt Merchant Services, we've been providing customized payment acceptance solutions to retail, ecommerce, and specialty merchants since 1992. Partner with Humboldt today and leverage our new Sales Partner Portal to review merchant processing and residual data, and (coming soon) submit and track online applications! Plus, take advantage of solutions for every merchant, all supported by:



Specialized chargeback reporting.



Multi-currency conversion.



A full suite of anti-fraud services.



A boutique client experience.

Isn't it time you got the personal service you and your merchants deserve?

Join the 25-year industry leader today.

855.767.0685 | HBMS.COM

Industries we specialize in:

Adult content · Bail bond issuers · Business opportunity · Buying clubs · CNP tobacco · Dating · Direct marketing · E-cigarettes · Firearms & ammunition and many more