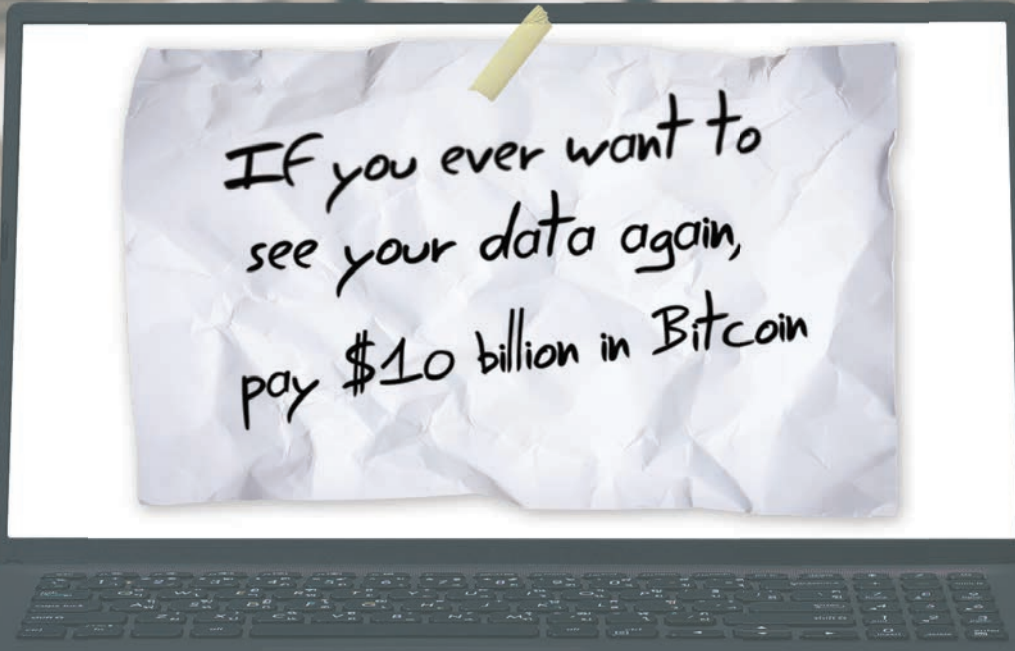


DIGITAL TRANSACTIONS

Trends in the Electronic Exchange of Value



IF you ever want to
see your data again,
pay \$10 billion in Bitcoin

RANSOMWARE'S LOVE NOTE FOR RETAILERS

How cyberattackers are targeting merchants' weaker defenses

Volume Nineteen, Number Three • DigitalTransactions.net • March 2022

ALSO IN THIS ISSUE:

Banks Pull Back on ATMs

Visa Puts the POS in a Cloud

Apple Ditches Dongles

Why QR Codes Need Specs

Everything You Need from One Family of Companies



VISIT US THIS SPRING!



**NORTHEAST ACQUIRERS
ASSOCIATION**

TRANSACT
POWERED BY ETA

Philadelphia
April 6-7

Las Vegas
April 12-14



The Companies of General Credit Forms are Ready to Meet all Your Point-of-Sale Needs

For more than 40 years GCF has been the leading single source for the merchant supplies industry — while remaining independently owned the entire time. As the industry changed, so did GCF. In reality, we often led the way. Today, our family of companies is your single source provider for business forms and distribution.

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

GCF
GENERAL CREDIT FORMS, INC.

Advanced
Labeling
Systems

GOLDEN
BUSINESS FORMS, INC.

PSI
Paper Systems

South Seas Data LLC

www.gcfinc.com • (888) GCF-NEWS

EXPERIENCE THE FUTURE OF COMMERCE

Shift4 is pushing commerce boldly forward across the world, and we want you to join us!



We offer an industry-leading partner program with lucrative revenue opportunities and a whole lot more, including:

- Best-in-class point-of-sale, mobile, and contactless technology solutions
- Disruptive pricing model to help you beat the competition
- Unmatched residuals and recurring revenue streams
- Upfront signing bonuses for you and your clients
- Customized marketing support and a dedicated sales support team
- 400+ POS/PMS integration partners to help you win business in new verticals

Visit shift4resellers.com to learn more

SHIFT **4**[™]

contents

MARCH 2022 • VOLUME 19, NUMBER 3

Ransomware's Love Note for Retailers

22

Cyberattackers think they've found an easy mark. They may be right.

THE GIMLET EYE Guess Who's Growing Fast?

4

TRENDS & TACTICS

6

Banks' Gift to Independent ATM Deployers

As banks pull back, independents are rushing to fill the void.

Silvergate's Deal for Diem Caps a Troubled Saga

The Facebook-initiated digital-currency venture has a new owner—and maybe better prospects.

Fee Transparency Helps Boost Seller Satisfaction

Suddenly, merchants are preferring banks to fintechs for transaction services.

PayPal Pays a Price

Analysts don't like its decision to pull back on user growth.

Plus, Security Notes asks whether the cops can put a cap on cryptocrime; and Payments 3.0 explains why the financial-services industry should regret its move to free checking.

ACQUIRING

13

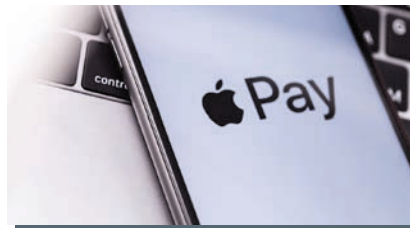
A Future in the Cloud

The Visa Acceptance Cloud will virtualize POS terminals. What will that mean for acquirers and merchants?



Cover Illustration: Elizabeth Novak, 123rf.com

Digital Transactions (USPS 024-247) is published monthly by Boland Hill Media LLC, 800 Roosevelt Road, Building B, Suite 212, Glen Ellyn, IL, 60137. Periodicals Postage Paid at Glen Ellyn, IL, and at additional mailing offices. POSTMASTER: Send address changes to Digital Transactions, P.O. Box 493, Northbrook, IL 60065-3553.



COMPONENTS

18

Look Ma, No Dongle

Apple's Tap to Pay has captured the industry's attention. Now the question is how far it can get with it—and how rivals will react.

M-COMMERCE

28

How to Get the Most Out of QR Codes

This new payment technology is spreading fast, but a common set of specifications is urgently needed to ensure global compatibility.

ENDPOINT

31

Fixing Open Banking's One-Way Street

Financial institutions have been cooperating with fintechs for years on data exchanges. But now banks need to get on the receiving end, says Sarah Grotta.

App Development Made Easier and More Secure

with the combination of MagTek hardware and Magensa Tools and Services.

Contactless

DynaFlex Pro BCR accepts swipe, tap, dip, and mobile wallet payments. SRED PCI PTS ready for P2PE environments.



TokenExchange

Touch free payments simplified with Magensa TokenExchange. Transactions made faster and easier with QR Codes and invoicing, protecting sensitive data.



Development

ISVs and VARs quickly customize their solutions with MagTek and Magensa's comprehensive drivers, APIs, and SDKs available for free on magtek.com.



Scan to Learn More!

Discover DynaFlex Family



FIND OUT MORE

☎ 562.546.6400
✉ sales@magtek.com
🌐 www.magtek.com

GUESS WHO'S GROWING FAST?

THE PANDEMIC HAS SPEEDED ADOPTION of the automated clearing house network for business-to-business payments, while transactions cleared and settled through the network on the same day they're initiated are booming, according to full-year 2021 numbers released early last month by Nacha, the governing body for the nationwide network.

We've written before in these pages about the growth—and expanded utility—of the ACH for payments. But because we're talking about a 48-year-old system, perhaps the story gets lost among all the glitter of newer and sexier payment methods.

So it's worth focusing again on the growth of the ACH, particularly in faster payments, peer-to-peer transfers, and other categories. All told, the ACH handled 29.1 billion transactions last year, up 8.7% from 2020. Dollar volume totaled \$72.6 trillion, up fully 17.4%. By contrast, Visa, the world's largest card network, processed 164.7 billion transactions last year worth \$10.4 trillion.

The biggest gainers on the ACH last year were peer-to-peer transactions, up 24.6% to 271.2 million payments, and B2B, up 20.4% to 5.3 billion transactions. Health-care payments followed closely with a 17.9% rise year-over-year, to 426.3 million.

But perhaps the biggest story at the ACH lies in the network's relatively new same-day payments category, which began operations in 2016. These payments totaled 603.8 million for the year, worth \$943.7 billion, representing increases of 73.9% and 105.1%, respectively.

The same-day category embraces both credits and debits, with debits claiming 55% of the transactions but 42% of the dollar value. Looked at another way, the same-day service processed 2.4 million payments daily last year worth \$3.7 billion.

Same-day isn't real time, but it may well meet the needs of most users for some time to come. And same-day ACH is expected to acquire even more momentum this month when a new rule extending the per-payment cap to \$1 million takes effect, a 10-fold increase from the old limit. The move, requested by banks, is one Nacha expects will widen the usefulness of the service.

The decision to raise the dollar limit follows other measures Nacha has made to facilitate same-day ACH. In March last year, the network added a new settlement window at the end of the processing day to extend the time in which banks can handle same-day items. As a result, the latest daily deadline for same-day ACH has moved to 4:45 p.m. Eastern Time, two hours later than the former cut-off. The move in part was a response to banks in the Pacific time zone that now have more leeway to enter same-day volume.

So don't be quick to neglect the massive ACH network when looking at faster—and newer—payment channels.

John Stewart, Editor | john@digitaltransactions.net

PUBLISHER Robert A. Jenisch

EDITOR-IN-CHIEF John Stewart

SENIOR EDITOR, DIGITAL
Kevin Woodward

CORRESPONDENTS
Jim Daly, Peter Lucas

ART DIRECTOR/PRODUCTION EDITOR
Elizabeth Novak

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 © 2022 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.

ROUND² *Point-of-Sale*

**Do you know where your
Sales Reps are?**



We do!
Round 2 CRM

Be part of the Round 2 POS Transformation.
Now recruiting Sub ISOs and
Agent offices for our solutions.

www.Round2POS.com

Visit our booth at a conference near you or contact us at Sales@R2POS.com

NEAA Conference
Philadelphia, Pennsylvania
April 6-7, 2022

SEAA Conference
Atlanta, Georgia
June 13-15, 2022

MWAA Conference
Chicago, Illinois
July 27-28, 2022

BANKS' GIFT TO INDEPENDENT ATM DEPLOYERS

As banks pull ATMs from underperforming off-premise locations, it is creating an opportunity for independent ATM deployers to fill the void, says a report from RBR, a London-based research and consulting firm.

The trend, which is being driven in part by banks' growing emphasis on providing cashless payments to their consumers, such as through mobile wallets and contactless cards, could open the door for independent ATM deployers to increase their market share, especially in the United States. Independent ATM deployers in the U.S. have deployed more than half of the country's 425,000 ATMs, according to RBR. Globally, independent ATM deployers accounted for 16% of the ATMs deployed in 2020, the firm said.

One reason independent ATM deployers are able to make ATMs deployed outside a branch location economically viable, when banks can't, is that the independents have a lower-cost business model, observers say.

"Independent ATM deployers, which already represent more than half of the nation's ATMs, often benefit when banks remove underperforming bank ATMs at locations that no longer make economic sense for a bank-operated ATM," Sam Ditzion, chief executive of Boston-based Tremont Capital Group, says by email. "Independent deployers have far more cost-efficient operating structures and can fill those voids left by bank ATM deployers."

One way independent ATM deployers can lower their operating costs is through a so-called merchant-fill strategy, which relies on the merchant to re-stock the ATM with cash as needed. "That saves on cash-in-transit visits," Rowan Berridge, an RBR associate, says by email. "This means that they can operate at a lower threshold than banks in terms of the usage levels needed to make the machines economically viable."

THE DECLINING BANK SHARE OF ATMS

(Worldwide deployment, in millions)



Source: RBR

Also helping independent ATM deployers in the U.S. to increase their share of off-premise locations is that, despite the rising popularity of cashless payment options the past two years, cash still remains strong in many regions.

“Different regions around the world have shown very different trends in cash over the past decade,”

Ditzion says. “The United States has a far more complex payments industry than most regions and demand for cash has been consistently resilient, even during Covid-19.”

As banks pull unprofitable off-premise ATMs, they are expected to focus on making their remaining ATMs more profitable. One strategy for this is greater levels of ATM shar-

ing and cooperation. “In the past, having their own large ATM fleets was seen as a competitive advantage,” says Berridge, who leads RBR’s annual global ATMs research.

Advanced software to help maximize uptime is another way banks can improve the economic viability of ATMs in their fleet, Berridge adds.

—Peter Lucas

SILVERGATE’S DEAL FOR DIEM CAPS A TROUBLED SAGA

Silvergate Capital Corp. last month confirmed widespread reports that it had acquired assets from the stablecoin venture Diem Group. The deal, valued at \$182 million in cash and stock, includes Diem’s intellectual property and “other technology assets related to running a blockchain-based payment network,” according to the announcement.

The La Jolla, Calif.-based bank, which has been working with Diem since the digital-currency venture moved to the United States last spring from its original headquarters in Switzerland, said it will use Diem’s technology to develop a dollar-based stablecoin it says its clients have been requesting.

“Through conversations with our customers, we identified a need for a U.S. dollar-backed stablecoin that is regulated and highly scalable to further enable them to move money without barriers,” said Allen Lane, chief executive of Silvergate, in a statement. “It remains our intention to satisfy that need by launching a stablecoin in 2022, enabled by the assets we acquired today and our existing technology.”

Silvergate’s technology includes a real-time payments service called Silvergate Exchange Network, which it intends to integrate with the Diem assets. “We have confidence in Silvergate’s ability to take Diem’s technology forward and transform the future of payments,” said Stuart Levey, chief executive of Diem Networks US, in a statement.

The deal includes payment of \$50 million in cash and more than 1.2 million shares of Silvergate stock,

valued at approximately \$132 million at market close Jan. 31. The bank says it also expects to incur roughly \$30 million in costs to integrate the Diem platform.

The Diem venture has the backing of some 26 corporations, including Meta Platforms Inc., formerly known as Facebook, which reportedly holds a roughly one-third stake. Other backers include major firms such as Coinbase, Shopify, Spotify, and Uber.

MONTHLY MERCHANT METRIC

Total Same Store Sales YOY Growth %

This is sourced from The Strawhecker Group’s merchant datawarehouse of over 3M 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 \$5M in annual card volume as well as Standalone Merchants Only.

Metric Definitions: (Only use definitions related to an individual month’s release)

Same Store Sales YOY Growth % - Annual volume change/growth of retained (non-attributed merchants with positive revenue and volume) accounts for given period divided by total portfolio volume from same period of the prior year

Note: Previous metric included all active merchants, those with positive revenue, whereas the new metric shown only includes merchants with positive revenue and volume.

Source: The Strawhecker Group © Copyright 2022. The Strawhecker Group. All Rights Reserved. All information as available.

Q4 2020		1.59%
Q1 2021		8.76%
Q2 2021		36.36%
Q3 2021		15.56%
Q4 2021		16.68%



Facebook spearheaded the launch of Diem, then known as Libra, in 2019 and recruited a wide range of firms to help finance and run the venture, including big payments firms like Mastercard, PayPal, Stripe, and Visa. But many of these companies backed out in the face of widespread criticism from governments around the world that saw the private initiative as a potential threat to their own efforts to develop and establish digital versions of their sovereign currencies.

Payments-industry veteran David Marcus, who had headed up an effort at Meta to develop a digital wallet for Diem, left the company in December. Last month, reports emerged that the association was looking to dispose of its assets.

The latest move follows an agreement Diem struck with Silvergate last spring in which the bank agreed to issue a U.S. dollar stablecoin for the association, an about-face from Libra's original mission to create a cryptocurrency tied to government securities and other assets. In May, the venture also announced it was relocating its headquarters to the United States from its original base in Geneva, Switzerland's banking hub.

But by the turn of the year, it was apparent Diem had reached the end of the road. "Despite giving us positive substantive feedback on the design of the network, it nevertheless became clear from our dialogue with federal regulators [in the United States] that the project could not move ahead," said Levey in his statement. "As a result, the best path forward was to sell the Diem Group's assets."

—John Stewart

FEE TRANSPARENCY HELPS BOOST SELLER SATISFACTION

After years of trailing fintechs such as Square Inc. when it comes to merchant satisfaction with payment processing, big banks find themselves atop the leader board, according to J.D. Power's 2022 U.S. Merchant Services Satisfaction Study.

Bank of America Merchant Services leads the way, posting a satisfaction score of 894 points out of a possible 1,000, up from 849 the prior year. Chase Merchant Services ranks second with a score of 879, up from 844 a year earlier. BofA and Chase ranked third and fourth, respectively, in the 2021 study (chart, below).

J.D. Power based its latest results on a survey of 4,406 small-business customers of 16 merchant-services processors in September and October of 2021.

But it's not just big banks that are posting higher scores with merchants. Fintechs are scoring higher, too. Square, which ranked first in the 2021 study, tallied a satisfaction score of 879, up 23 points from a year earlier. And PayPal Holdings Inc. posted a score of 877, a gain of 25 points.

Despite these higher scores this year, Square and PayPal slipped to third and fourth place, respectively,

HOW THE ACQUIRERS RANK

(Top 10 in merchant satisfaction scores, based on a 1000-point scale)

	2022	2021
Bank of America	894	849
Chase Merchant Services	879	844
Block (Square)	878	857
PayPal	877	852
Wells Fargo Merchant Services	876	833
Stripe	872	841
Industry Average	859	836
Elavon	854	836
Global Payments	854	824
North American Bancard	854	815*
Shopify	849	853*

*Small sample size. Source: J.D. Power

in the latest study after finishing first and second in 2021. Overall, the average satisfaction score in the 2022 study was higher, totaling 859 points, up from 836 in 2021.

The key factors in the general turnaround for merchant processors are improved communication about how merchants can reduce processing costs, greater fee transparency, and faster settlement. Overall satisfaction with the cost of service increased 33 points in 2022, and satisfaction with service interaction increased 32 points, according to the survey.

“When it comes to processing technology, satisfaction scores have traditionally been good because the technology works like it is supposed to. It’s other areas of the business, such as cost of service and service

interactions, that have not scored as well. But now small businesses say they are seeing improvement in those areas,” says Paul McAdam, senior director of banking and payments intelligence at J.D. Power.

Increased speed for merchant payouts prompted 34% of respondents to say payment was faster than they expected. In addition, 65% of small businesses say they’ve received faster funding, so card payments are settled or posted same day or on non-business days, up 14 percentage points from 2021.

“Faster settlement times are a satisfaction booster for merchants, especially for restaurants, construction companies, and tradesmen,” McAdam says.

Processors’ responses to the pandemic also earned goodwill among

small businesses, with 73% saying they are aware of at least one proactive measure their merchant-services provider has taken in response to challenges caused by Covid-19.

This in turn has driven a 71-point increase in satisfaction with cost of service, the study says. Specific actions taken by providers include discounted products and services, updated fraud controls, and faster funding-turnaround times, according to JD Power.

Merchants also reported higher satisfaction with service via phone. This measure rose 32 points from the prior year. “We also saw a higher satisfaction level with the service representative,” McAdam says. “These are all good things to see.”

—Peter Lucas

eProcessingNetwork.com

The Everywhere Processing Network®

800-296-4810

Contactless/NFC

PIN Debit

Inventory

Cash Discount

LEVEL II & III

Multi-Merchant

QuickBooks® Sync



PAYPAL PAYS A PRICE

As all payments companies know, some active accounts are more active than others. Last month, PayPal Holdings Inc.'s top executives made it plain the company's 2022 priority is to emphasize—and pour money into promoting—accountholder activity.

“The shift is, we're not going to throw marketing dollars at low-value customers coming in,” declared chief executive Dan Schulman during an afternoon session to discuss his company's fourth-quarter 2021 results. That means, he said, that “we are shifting our emphasis toward engagement.”

But the market saw the shift in emphasis as a shift away from growth, and savaged PayPal's stock accordingly. The company's share price, which began the year at just over \$188, was still trading at just shy of \$116 by mid-February, two weeks after the earnings release.

User engagement is a metric Schulman has watched closely since taking over as the payments giant's top executive more than six years ago. Now, with PayPal having weathered the worst the pandemic could throw at it, and with e-commerce activity stronger than ever, he's looking for ways to get more revenue—and potential profit—out of PayPal's most active users. “The vast majority of our volume comes from one-third of our customers,” said chief financial officer John Rainey during the call.

PayPal measures engagement in terms of transactions per account, and here the trend is positive. Overall, the active user base performed 45.4 transactions per account in the fourth quarter, up 11% from the final quarter of 2020. That was with

49 million net new active accounts added to bring the total to 426 million. Payment volume jumped fully 23% year-over-year to \$340 billion in the quarter. Volume for the full year totaled \$1.25 trillion—exceeding the trillion-dollar level for the first time in the company's 22-year history.

The new emphasis on customer engagement may already be paying off at the bottom line. PayPal posted a transaction take rate—the percentage of dollars it keeps on each transaction—of 1.88% in the quarter, reversing a slide that had seen the rate dwindle from 2.06% in the third quarter of 2020 to 1.81% a year later.

Supply-chain issues have hampered cross-border traffic for PayPal, but the company is weathering the latest impact of the pandemic, the top executives said. “It's clear to me we are in a significantly stronger position than when we entered the pandemic,” Schulman said.

Another positive is the early performance of PayPal's so-called super app, which launched last sum-

mer. The app supports an array of payments, shopping, and financial features and represents the company's first complete redesign of its app in seven years. It also enables cryptocurrency transactions. “Our super app is showing extraordinary early results,” Schulman said, pointing out the app generates twice the average revenue per active account.

In the highly popular buy now, pay later space, PayPal ended the year with \$7.9 billion in payment volume, 1.2 million merchants, and 12.2 million consumer accounts across eight countries.

Across the company, PayPal reported 426 million active accounts for 2021, up 13% year-over-year, including 34 million merchants. The company added 9.8 million active accounts in the fourth quarter alone, including 700,000 merchant accounts. The fourth-quarter total includes 3.2 million consumer accounts that came to PayPal in October via its \$2.7-billion acquisition of Paidy, a Japanese buy now, pay later provider.

Revenue for the quarter totaled \$6.9 billion, up 25% year-over-year.

—John Stewart



CAN THE LAW TAME CRYPTO CRIME?

EVEN CRYPTO BUSINESSES that keep saying crypto crime is tolerable recently had to acknowledge a whopping \$14 billion in reported criminal crypto activity occurred in 2021. The true figure is at least an order of magnitude higher, since many ransomware victims don't even report the crime.

The sad reality is that criminal empires have never had it so convenient, financially speaking. Drug trafficking, human trafficking, illegal arms sales, blackmail, and extortion of all kinds are mostly using Bitcoin as a shield, keeping one step ahead of the law. Yes, there are millions of law-abiding citizens trading with Bitcoin, and some see a handsome profit. But it is time for these honest traders to admit that, by taking part in the decentralized trade, they give aid and comfort to the destructive forces in society.

And it is not needed. Privacy is perfectly achievable with coins that are administered by a registered entity subject to the law of the land. Much as cash leaves the bank, moves around through unknown traders, and then is deposited by someone, somewhere, so can digital coins transact cash-like among anonymous traders, with the mint identifying only the purchaser and the redeemer. We already have the technology to establish a good balance between privacy and the law (for example, BitMint*LeVeL).

BY
**GIDEON
SAMID**

gideon@bitmint.com



Decentralized money is considered by common wisdom to be out of reach of the law. After all, you can't sue a protocol. Indeed. But you can outsmart a protocol. It's time for the law to be as imaginative as its targets.

**You can't sue a protocol.
But you can outsmart it.**

Bitcoin relies on the continuous attention of its traders to the notorious ledger of payments. It would be fair, therefore, to require the traders to peruse an FBI-alert crypto ledger. This ledger would list Bitcoin accounts that have been mentioned in a lawsuit. For example, a merchant paying ransom to regain its data might sue the owner of the receiving account. If that owner can take money anonymously, it should also be declared as a defendant in a lawsuit –owner identity unspecified.

The owner, perusing the FBI-alert ledger, will have the option to get out of the shadows and defend itself. If it doesn't, the trial will proceed on the merits of the complaint. If the court rules against the unknown

accountholder, the account will be added to a second ledger: the FBI-wanted ledger.

Over time, money from the condemned account will traverse from one account to the next (all recorded on the Bitcoin ledger). At some point, the current account holder will surface with its identity (for example, in proving that a bank deposit it made is a legitimate Bitcoin profit). When this identity is so exposed, the law will see that some of this money came from a condemned account, and confiscate it.

The very prospect of this confiscation will prompt each Bitcoin trader to check the FBI-wanted ledger to see if any payment made to them has a history of having been owned by a condemned account. If so, the payee will reject it.

And this is where the law flexes its muscles. Ransomware artists collecting their criminal fortunes will suddenly realize their money is no good. No one will want to accept it!

Now of course these wily criminals will think of something. They always do. But it is time for the good guys to use their imagination and show some determination. Suing an anonymous account may require administrative accommodation, regulatory accommodation, or even legislation. Let's rise to the challenge. The destructive impact of Bitcoin-aided crime is motivation. I hope an enterprising lawyer will take this baton and run with it! **DT**

HOW FREE CHECKING DOGS FINANCIAL SERVICES

THE ENTIRE FINANCIAL-services industry shot itself in the foot with free checking.

Free checking taught customers that they should not pay any fees for the services they receive from banks and other financial companies. The attitude is, “Why should I pay to access my own money?” Since these same customers may also be some of the people who work at the regulatory agencies, it is not hard to see how this attitude would start shaping the regulatory climate.

On Jan. 26, the Consumer Financial Protection Bureau released a “Request for Information Regarding Fees Imposed by Providers of Consumer Financial Products or Services.” The Bureau made up for the bland title in its press release, saying the request was the start of an “an initiative to save households billions of dollars a year by reducing exploitative junk fees charged by banks and financial companies.”

In its filing, the Bureau gives the example of “resort fees added to hotel bills and service fees added to concert ticket prices” as example of junk fees. It then goes on to suggest that things like card-replacement fees might be an example of this.

The apparent underlying assumption of the RFI seems problematic. It seems to assume virtually any



BY BEN JACKSON

bjackson@ipa.org

fee—whether it comes on a deposit account, a card, or a concert ticket—is a junk fee, and too high. It ignores the reality that all of these products cost money to offer, administer, and protect.

Maintaining payments networks, online and mobile banking platforms, and ATM networks has a cost. Securing those systems from hackers, and preventing social engineering and friendly fraud, has a cost. Providing cardholders with a zero-liability guarantee has a cost.

Perhaps infrastructure does not resonate as a reason to charge fees. To put a human face on it, should customer-service agents work for free? In most cases, financial-services companies have people ready to help someone with a problem 24 hours a day, seven days a week, whether the customer needs them or not. What ensures those workers a living wage?

One example that the RFI gives as a possible “junk fee” is a charge for card replacement. It says this fee may be a “surprise” or “inflated.” Does anyone expect that a plastic card with an encoded magnetic stripe and programmed chip can

be made, personalized, and put in a customer’s hands at no cost?

The RFI starts with the assumption that any fee is excessive. It asks “what fees exceed the cost to the entity that the fee purports to cover” and “What types of fees for financial products or services obscure the true cost of the product or service by not being built into the upfront price?” It returns to the original notion, implanted by free checking, that all fees are too much.

How would an individual customer know what the costs are of providing a service? Also, focusing on an upfront price distorts the conversation further. Should people pay upfront for the possibility of replacing a card, or should only those who lose a card be forced to pay for a replacement?

Fees may get out of whack from time to time, or a particular company might get greedy. But that’s not a reason to keep products out of the hands of consumers through excessive regulation. Making things free is what got us into this mess. We need to return to first principles and look at both sides of the balance sheet to conduct meaningful analysis that protects consumers. No judgment can be made about whether a fee is reasonable without a deep look into a product’s operating costs. **DT**

acquiring

A FUTURE IN THE CLOUD

The Visa Acceptance Cloud will virtualize POS terminals. What will that mean for acquirers and merchants?

BY KEVIN WOODWARD

THE DAWN OF a new era for point-of-sale terminals may be upon the payments industry with the announcement earlier this year of the Visa Acceptance Cloud. The platform aims to move to a cloud-based platform transactions that have required dedicated software on point-of-sale terminals.

This capability has been proven for years—think semi-integrated point-of-sale systems connected to POS terminals—and its application to standard POS terminals and Internet of Thing devices has the potential to broadly expand what might be considered a payment-acceptance device.

Though some analysts view the acceptance cloud as a further adaptation of devices and acceptance, it remains a new way of thinking about a stalwart of the payments industry. And, as with any change, there are questions about the potential impact.

First, just what is the Visa Acceptance Cloud? Visa says the platform removes the need for payment-processing software to be embedded in each hardware device to be universally accessible in the cloud. The card brand says the platform expands beyond its Tap to Phone technology, announced in 2020. Tap to Phone made it so Android smart phones and tablets could be used as contactless POS terminals with no additional hardware.

Tap to Phone was in use on more than 300,000 devices across 54 countries as of Dec. 31. Tests of the Visa Acceptance Cloud are ongoing in North America, South America, Europe, Africa, Asia, and Australia.

In addition to payment acceptance, Visa Acceptance Cloud incorporates buy now, pay later services, fraud management, advanced data analytics, and Rapid Seller Onboarding, a merchant-onboarding service in Visa's Central and Eastern Europe, the Middle East, and Africa region.

BROADENING ACCEPTANCE

Details are sparse regarding Visa Acceptance Cloud, including how it



works, which devices are eligible, when it will be broadly available, and how it will be distributed. Visa declined to comment further on these questions.

Still, it seems clear that, even without many available details, the Visa Acceptance Cloud could be transformational. “Any time you see innovation that broadens acceptance, it is compelling,” says Ginger Schmeltzer, strategic advisor at the Boston-based consultancy Aite-Novarica. “It makes it easier to pay, which I always think is so important.”

Using as an example the growth in easier checkout experiences for online shopping, Schmeltzer says each iteration of technology that allows merchants to accept payments more easily, and for consumers to pay more easily, results in a more streamlined and better consumer experience. “It’s taking friction out of the process,” she says.

But, beyond enabling smoother transactions, the Acceptance Cloud also could make it easier for third parties to integrate payment functionality befitting their market behaviors and end users, suggests Cliff Gray, senior associate at The Strawhecker Group, an Omaha, Neb.-based advisory firm.

“It’s largely the SoftPOS model, similar in approach to semi-integrated,” Gray says, “since all the handling of sensitive data has been

moved off the resident hardware, the underlying certification requirements have been removed to the cloud, freeing the merchant to bring their own equipment to the party.”

For example, Ford Motor Co. might use a generic Android operating system in its vehicles and another company’s near-field communication kernel and “have no concerns about PCI and other certification requirements,” Gray says. “They can go to market more quickly.”

CHANGING MODELS

Going to market quicker, making payment acceptance easier for consumers and merchants, and providing better security for transactions are the expected payoffs from most improvements to the payments process. But what does the Visa Acceptance Cloud present now?

For one, more merchants might be able to use commercially available, off-the-shelf devices that are NFC-enabled with an app only—no plug-in dongle. Companies like MagicCube Inc. launched its cloud-based acceptance platform earlier this year and just in February Apple Inc. finally capitalized on its 2020 acquisition of Mobeewave Inc. by launching Tap to Pay with iPhone with a similar capability (for more on this, see page 18). “NFC is pretty standard now,” Gray says.

“The point of sale has evolved,” Schmeltzer says. “We’re already moving away. The acquirers already have to change their models. I don’t think this was unexpected.”

As chief technology officer at Paya Holdings Inc., an Atlanta-based payments provider, Balaji Devarasetty has witnessed the ongoing adoption of cloud technology for payments. As EMV became widespread in the United States, POS software developers needed a secure way to capture payment card data without housing it in their applications.

The semi-integrated POS model was ushered in as a way to use a POS terminal to capture the data, send it to the cloud for processing and return the authorization decision to the software, minimizing PCI-compliance matters and reducing risk to the merchant.

“The natural progression was the terminal had to be connected to the cloud, as well,” says Devarasetty. Then, as the EMV rollout continued, NFC was built into the new EMV terminals merchants were using. That trend evolved into a smart POS terminal, like GoDaddy Inc.’s Poynt device, he says. Now, the smart device has become the phone itself.

Will that be a big change for acquirers? Probably not. “Cloud processing for POS transactions, it’s already happening with the advent of Clover, Square, Toast, Shopify, and other restaurant POS systems,” Devarasetty



No panicky rush among acquirers to change their models.

—GINGER SCHMELTZER, STRATEGIC ADVISOR AT THE BOSTON-BASED CONSULTANCY AITE-NOVARICA

» LEVERAGING TECHNOLOGY TO AMPLIFY PROFITABILITY

If you're looking for ways to pay, get paid, optimize and grow your ISO, First American by Deluxe specializes in payment technology and business solutions to help you do just that.

As former business owners, direct merchant services salespeople and payments industry experts, we understand the challenges you face, and we deliver meaningful services to help you grow your merchant portfolio.

» Want a go-to-market strategy that supports your business today and tomorrow?

We can help.

» Searching for POS, ecommerce and software integration solutions to best serve your merchants?

Look no further.

» Need an HR & Payroll program to help your ISO and your merchants manage employees?

Consider it done.

From startups to well-established businesses, our strategies, our products and our solutions are designed to give you a competitive edge. **Put us to work for your ISO today.**



sales@first-american.net | 866-464-3277

www.first-american.net

Learn more at

ETA Transact in Las Vegas, NV
April 12-14





With reduced concerns about certification demands, merchants using Visa Acceptance Cloud could go to market more quickly.

—CLIFF GRAY, SENIOR ASSOCIATE AT THE STRAWHECKER GROUP

says. “These are already hosted in the cloud. That is not new. What I’m seeing is acquirers also shifting more to the cloud.”

Big processor Global Payments Inc., for example, said in 2021 it was moving its merchant-acquiring technology to Google Cloud. And Stripe Inc., which is working with Apple on application to run on iPhones for the new Tap to Pay service, uses Amazon Web Services.

‘THE CLOUD HAS EVOLVED’

Acquirers have already proven their adaptability, and expectations are that will continue with moving POS transactions to the cloud. There is no panicky rush among them to change their models, Schmeltzer says. “It just accelerates, pushes it farther along,” she says.

A broad adoption of the Visa cloud technology, which is expected and likely will yield similar services from the other major U.S. card brands, may force acquirers to adapt their hardware-leasing and other revenue models, Gray says, “as well as all the deployment implications of merchants who no longer require any hardware.” American Express Co., Discover Financial Services, and Mastercard Inc. did not respond to inquiries from *Digital Transactions*.

The chief benefit for a merchant is that the business may not require

a dedicated device resting on the countertop. It will just need an app. “It means I don’t need any additional hardware,” Schmeltzer says. “It becomes much less of a hurdle to get there.”

And for many smaller merchants, the technology could allow them to have the latest payment-acceptance technology, which might have been too expensive or too demanding otherwise. “The merchant can stay nimble,” she says.

For consumers, it can afford them flexibility in how and who they can pay electronically. As an example, a parent might just tap her card or mobile phone against a swimming instructor’s phone to complete a payment. “It becomes more [appealing] when I as a consumer have much more flexibility in how to accept payment,” Schmeltzer says.

The other payoff for merchants, as it has been with the semi-integrated model for POS software, is much of the risk, along with the merchant’s PCI-compliance requirements, could be reduced.

In years past, cloud providers might not have been able to meet regulatory requirements for compliance as easily as today, Devarasetty says. “But now the cloud has evolved,” he says. “The Amazons and Googles have become smart and can tell exactly where your data is.”

And PCI compliance might be lessened, since no card data is handled onsite. Cloud-based point-of-sale “completely obfuscates the [primary account number] and data around it from the merchant environment,” notes Gray. “That’s just one example of the advantages of cloud-based POS systems. They take the data-security management off the merchants. They have to certify the NFC kernel.” The NFC kernel is the key piece of code enabling NFC interactions.

‘ACCELERATING CHANGE’

If the barriers to acceptance are lower because of cloud-based POS transaction processing, that could translate into more embedded payments in more places, such as automobiles and other Internet of Things objects.

At its core, the Visa Acceptance Cloud is an acknowledgement of the advances in payment technology, merchant acceptance, and consumer expectations. The payment-acceptance component is important, but it’s the value-add services surrounding it that may harbor the most potential.

“It’s a matter of what part of that package the actual acceptance piece holds,” Schmeltzer says. “The value-adds are much more important than the actual transaction itself. It’s just accelerating change that was already happening.” DT



Customization That Pays

Grow your portfolio with payment programs tailored to your business.

At Merrick Bank, we make it our business to know your business—and we tailor our programs to meet your goals and objectives.



Retail ISOs

- Fast start bonus
- Auto approval
- Lifetime residuals
- Extensive MCC capabilities



Wholesale ISOs

- Auto approval
- Multiple processors
- Portability
- Extensive MCC capabilities



PayFacs

- Easy integration
- Fast setup
- Recurring revenue
- More control

Merrick Bank[®]
Merchant Acquiring

Contact us today!

(844) 320-7100

MerrickBankAcquiring.com/Contact



LOOK MA, NO DONGLE

Apple's Tap to Pay has captured the industry's attention. Now the question is how far it can get with it—and how rivals will react.

BY JOHN STEWART

APPLE INC. STIRRED up the point-of-sale industry last month with an announcement that it will introduce within a few months technology that will enable merchants to accept Apple Pay and card transactions on an iPhone without any card-reading dongle or other attachment.

It turns out, though, that the development, for all its deep portents for the POS business, may have been less a surprise than many may have thought.

The computing giant has been working on this product, dubbed Tap to Pay, at least since the middle of 2020, and perhaps for some time before that. In August that year,

news emerged that Apple had bought a Montreal-based company called Mobeewave Inc., which had developed just such technology for handsets from Samsung Electronics Co. Ltd.

Apple wanted the technology enough that it reportedly shelled out anywhere from \$120 million to \$150 million for Mobeewave in a deal that could have closed months before the news went public.

The Samsung product included the near-field communication link Tap to Pay will depend on. But Mobeewave made its proposition even more interesting—and particularly valuable to a certain tech titan looking to expand into the point of sale beyond Apple Pay—by adding to the Samsung proposition in January that year a capability that allows a merchant to enroll and begin accepting payments within 10 minutes.

Apple's move took the technology out of the hands of Samsung—a major handset rival—and gave Cupertino a key to the fast-growing small-merchant market. Indeed, snapping up Mobeewave laid the groundwork for a “micro-merchant play,” says Chip Kahn, founder and chief executive at Boomtown Inc., a POS services provider. The ease of making payments renders Tap To Pay, he says, “almost like a card-present Venmo.”

Apple said last month that Tap to Pay will work on the iPhone XS,



launched in 2018, and later models, so there should be plenty of potential handsets in the hands of those small businesses (see chart on page 20).

A SALIENT STRATEGY

Nobody is so bold as to predict the demise of the conventional POS terminal. Makers of these devices, after all, are showing strength again following the worst impact of the pandemic. One example: Verifone, long a stalwart in this business, which is seeing double-digit revenue growth.

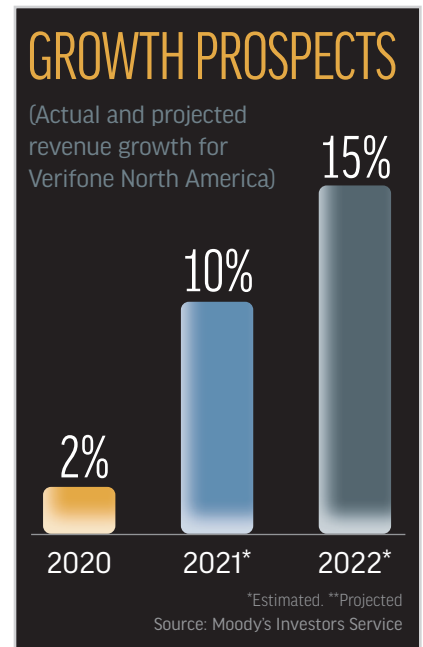
But the surge in business startups among micro-merchants, particularly as the pandemic caused many workers to try their hand at running a shop, presents a rising opportunity for technology like Tap to Pay.

Of the 32 million U.S. small businesses, an estimated 23 million employ 20 or fewer people. Numbers on how many of these firms are e-commerce rather than brick-and-mortar businesses were not readily available. Suffice it to say a good many are both.

A partnership Apple forged with Stripe Inc. to offer processing for Tap to Pay could make it even easier for small businesses to adopt the iPhone for payments. This is a particularly salient strategy given Stripe's strength among independent software vendors, the players that weave payments capability into business software.

"Stripe is heavily courting the ISV space, and has been for years," notes Don Apgar, director of merchant

services at Mercator Advisory Group, a Marlborough, Mass.-based consultancy. And with the onset of cloud



The payments market is large and fragmented.

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



Concise, clean interface is **easy to navigate**

Breaking news from the payments market, posted daily

Calendar of industry events

Complete current and past issues of **Digital Transactions magazine**

Detailed listings of payments market suppliers

13 years of payments news and analysis



computing at the point of sale, the ISV channel is an inevitable pathway to market.

Apple's thrust into POS technology has also led many observers to speculate that the player with the most to lose from Tap to Pay is Block Inc., whose Square card readers emerged more than a decade ago to fill the same gap Apple is now apparently targeting—a need for simple and fast payments acceptance at corner shops, food trucks, diners, and other small sellers.

‘THE NON-SEXY STUFF’

But the whole acquiring question surrounding Apple's latest product is a bit too murky to suit some observers. Apple hasn't talked "about the non-sexy stuff," observes Bradford Giles, senior vice president of marketing at the big terminal maker Ingenico Group, who contrasts the openness of the Android operating system with the traditional closed culture at Apple. "Are they going to open [Tap to Pay] to all acquirers?"

Android has been adopted by a wide range of device makers over



"In payments, open always wins."

—SAM SHAWKI, MAGICCUBE INC.

the years because of its open environment. But at the same time, these players may have the most to lose from Apple's latest gambit, Giles says. "We'll feel some impact, we'll feel it a little bit, but we're not overly concerned," he says. Apple did not respond to written questions from *Digital Transactions* regarding Tap to Pay.

One developer that has been making hay with an Android-based version of Apple's latest POS technology is Santa Clara, Calif.-based MagicCube Inc., founded in 2014 by former Visa executive Sam Shawki to enable merchants to take card transactions on everyday mobile devices. Now, with Apple's announcement, "our phones have been ringing," Shawki says.

No wonder. A survey sponsored last fall by the processor NMI indi-

cated 34% of small and medium-sized businesses in the U.S. market still don't accept contactless payments. Some 300 small businesses and 1,000 consumers were included in the survey.

Now the race is on to ease the way to contactless for those merchants, and Shawki argues he's in the best position to win it. That's because MagicCube's latest gambit is i-Accept Cloud, a service that can run on both Android and iOS devices.

"We're giving everyone the freedom to run on anything. In payments, open always wins," Shawki says. Rather than locking themselves into Apple's platform, he argues, merchants "should be talking to me because I can give you the Android market [also]. We have ubiquity."

Still, Apple's entry with both feet into Shawki's market may raise some questions that could go unanswered for some time. Shawki, for example, predicts that the impact on Square's device base will be negligible, particularly if Apple restricts Tap to Pay to iOS. But Apple is likely to impose what he calls a "tax"—a levy above interchange "on its own behalf. I don't know who's going to absorb it. It could be the merchant."

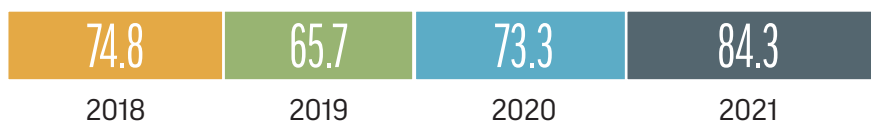
Executives with other device makers are inclined to agree. "Apple will keep taking a bigger part of the apple," says Chris Lybeer, chief strategy officer at Atlanta-based Revel Systems. "There's no rocket science here. Apple controls the device." **DT**

TRACKING THE IPHONE

(Active units in the U.S. market, in millions)



(Sales in the U.S., in millions)



Source: Business of Apps



wholesale payments

The last partner you will ever need.

There are many partners to choose.

Why choose Wholesale Payments?

- Unmatched Support and Training
- 2 to 3 Qualified Pre-Set Appointments Per Day
- Portfolio Purchases up to 45X
- Latest Technologies for Merchants
- Transparent and Robust Back Office for our Sales Partners

Call today about our
**DAILY, QUALIFIED
Appointments &
\$50,000** Fast Start
Bonus!



**Call or
Email Us
TODAY!**

806.642.4949

partners@wholesalepayments.com

RANSOMWARE'S LOVE NOTE FOR RETAILERS

The past two years have seen merchants become frequent targets of ransomware attacks, largely due to their weaker cybersecurity practices. The threat only promises to get worse.

By Peter Lucas



FOR CYBERCRIMINALS, RANSOMWARE attacks are easy money. To cash in, hackers need only plant malware on a target's network to gain entry. Once inside, criminals can identify personal consumer data, lock up the data using encryption, and then send the business a digital ransom note threatening to erase or publish the data online unless the ransom is paid.

Upon payment, which typically takes place by depositing cryptocurrency in the attacker's crypto wallet, the victim receives the key to decrypt the data.

Considering that ransom demands can range from five figures to millions of dollars, and that attacks will target multiple companies at once, that's not a lot of work for a lucrative payday. Further enhancing the appeal is that cybercrooks don't have to assume the risk involved in stealing and selling data, a crime that puts them at greater risk of being caught by law enforcement.

"Criminals can make so much money from ransomware, they only need to work a work a couple of months a year, if they choose," says Gideon Samid, chief technology officer for McLean, Virginia-based BitMint, a digital currency. Samid writes the monthly "Security Notes" column for *Digital Transactions* (page 11).

No surprise, then, that ransomware has become one of the fastest-growing cybersecurity threats. In 2021, ransomware attacks represented 21% of reported data breaches, up from 17% in 2020, according to Risk Based Security Inc. Overall, ransomware attacks hit a remarkable 37% of all businesses globally last year, according to the PCI Security Standards Council. Of these, 32% paid a ransom demand, the Council says.

Ransomware has become so problematic the Council in February issued a joint bulletin with the National Cybersecurity Alliance warning about the growing threat. "These cyber threats are real and require immediate action to better protect against these ongoing criminal activities," says Lance Johnson, the Council's executive director.

Low-Hanging Fruit

Since the start of the Covid-19 pandemic in 2020, retailers in particular have come under severe attack. As of August 2021, 44% of retail organizations had been hit by ransomware in the last year. Of these, 54% said the attackers succeeded in encrypting their data, according to the latest figures from cybersecurity firm Sophos Ltd. The average ransom payment was \$147,811, Sophos says.

There are myriad reasons why retailers have become such prime targets. First, many have experienced explosive growth in online sales during the pandemic, which in turn prompted those with a modest e-commerce presence to expand that part of their business or add an e-commerce channel if they lacked one. But, by expanding their e-commerce operations, retailers unwittingly opened up more avenues of attack for hackers.

Furthermore, some retailers expanded their e-commerce operations so rapidly that appropriate cybersecurity was left behind, says Daniel Tobok, chief executive of Cytelligence, a Toronto-based cybersecurity firm.

Another contributing factor is that merchants typically don't spend as much on cybersecurity as a financial institution or payment processor does, even though they house reams of personal consumer and account data. In many cases, retailers' cyber defenses meet payment card industry (PCI) security standards, but they rarely extend beyond those minimums.

Retailers may struggle to justify the return on investment from more extensive cybersecurity spending and instead prefer to view security as a one-time investment. And some retailers operate legacy systems that are costly and time-consuming to update, while others face the challenge of integrating disparate systems from a recent merger or acquisition.

But the most telling reason for retailers' susceptibility to attack is that criminals know they are likely to pay. In 2020, 32% of retail organizations whose data was encrypted as part of a ransomware attack paid the ransom to recover their data, according to the latest figures from Sophos.

Complicating matters is that many retailers can't afford to have their businesses shut down for any length of time. Paying the ransom is often seen as the easiest and most cost-effective path to getting back in business quickly, cybersecurity experts say. Another key factor in the decision is whether the company has insurance covering a ransomware attack.

"Whether or not to pay a ransom is a business decision," says Dan Holden, vice president for cybersecurity at Austin, Texas-based e-commerce platform provider BigCommerce Inc. "It's not uncommon for retailers to figure the [return on

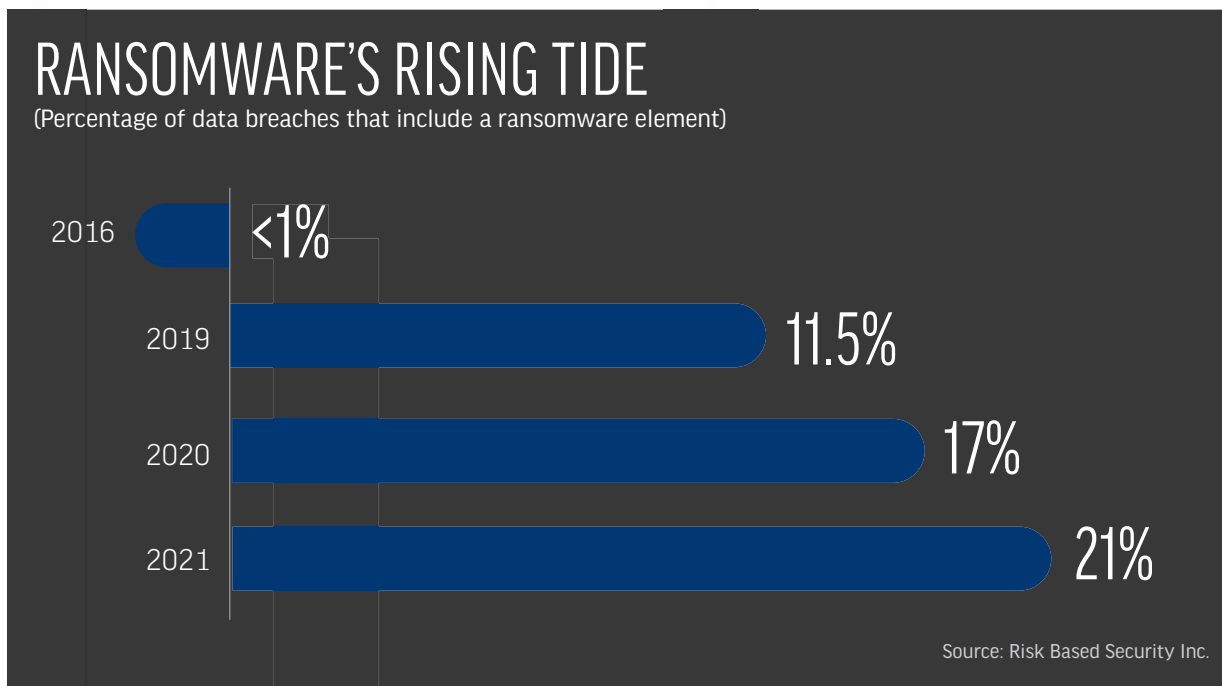
investment] of paying vs. not paying, especially if they have no hard-and-fast rules in place for dealing with a ransomware attack."

For some retailers, indeed, the decision whether to pay a ransom has been made in advance, which is why they have pre-funded cryptocurrency wallets at the ready. Not surprisingly, criminals know this, experts say.

"This strategy has unwittingly made it easier for criminals to launch attacks, because cryptocurrency is how they want to be paid [because of the anonymity it provides]," says Tari Schreider, strategic advisor for the cybersecurity practice at Aite-Novarica Group, a Boston-based consultancy. "Ransomware attackers view retailers as low-hanging fruit."

A retailer initially may refuse to pay the ransom, but cybercrooks have contingencies in place. One tactic is to shame the retailer on social media by publicizing the attack and the retailer's unwillingness to pay the ransom. Such tactics can damage the target's brand and drive away repeat customers, who may fear their data is inadequately protected.

"Criminals have multiple avenues for coercing people into paying beyond just encrypting data," says Schreider.



NORTHEAST ACQUIRERS ASSOCIATION

2022 CONFERENCE

APRIL 6-7

NEAA Charity Poker Tournament is back!

Don't miss your chance to gamble for a great cause and prizes, April 6th, 9pm

Hosted by Shift4



Serving the needs for all merchant acquiring payment professionals.



Education

From industry trends and product features to lessons learned both here and abroad. We provide you with all the late breaking news, including legislative information impacting you and your customers.



Partner Opportunities

Looking for complementary products and services to offer your clients? We bring together the newest and best vendors with innovation as the primary focus.



Networking

You're not on a island by yourself. Together with peers, learn how others expand their client base, what new products are available and how to best leverage them to bring your business to the next level.





"Give me liberty! Give me NEAA!"

ABOUT NEAA

Our annual conference provides an educational forum that covers the most current industry issues, trends and topics. We provide economical access for attendees to meet with the companies that are the front-runners in developing the latest payment technologies, solutions and products.

Register Here

 Philadelphia, Pennsylvania

 www.northeastacquirers.com



Watering Holes

Further fueling the rise of ransomware attacks is advances in the technology itself, which has made the crime even more financially attractive.

One of the biggest game-changers to emerge is ransomware-as-a-service (RaaS), which allows larger criminal organizations to sell their proprietary ransomware to affiliates in exchange for a monthly or one-time licensing fee or a percentage of each ransom paid to the affiliate. RaaS is a criminal variation of the increasingly popular software-as-a-service (SaaS) business model.

The rise RaaS has made it ridiculously easy for criminals to get in the game, which has only exacerbated the ransomware threat.

Indeed, “cybersecurity experts have reported that almost two-thirds of 2020 ransomware attacks came from cybercriminals operating on a RaaS model,” says Marwan Forzley, chief executive of Veem, a San Francisco-based online-payments platform.

“It is also predicted that RaaS will rise in 2022 as attackers with non-technical knowledge can carry out the attack more easily by purchasing ransomware kits,” Forzley says. “What makes it worse is that some ransomware creators provide the ransomware kits for free in exchange for a share of the profit.”

A RaaS kit can be readily purchased on the dark Web. With the kit, a novice attacker can open and pay for an account using Bitcoin, then get access to programming code and instructions for easily creating a malware program. The most sophisticated RaaS operators reportedly offer portals that let their subscribers see the status of infections, total payments, total files encrypted, and other information about their targets, as well as provide access to support, user communities, updates, and other benefits.

The most common attack vector into a network is through phishing. Phishing attacks download malicious software from email sent by a criminal masquerading as a trusted entity to an unsuspecting employee when the message is opened. Once the malware is activated, criminals can gather employee

usernames and passwords that can open doors to sensitive data within the network, all while avoiding detection.

Other types of attack include downloading malware to a computer when an employee visits an infected Web site; fake service scams, such as technical-support ploys that launch malware to the employee’s computer when the user clicks on the service message or pop-up window; and malicious links or attachments in an email.

Attacks can also be launched against vendors connected to a targeted company’s network. The vendors then unwittingly transfer the malware to their trading partners.

One of the more exotic tactics, though, is a so-called watering-hole attack. This tactic, which got its name because criminals launch it where potential targets are likely to congregate on the Internet, poses a considerable threat because it is difficult to detect. The attacks can target individuals, a group of people, or an entire organization. When the intended target arrives at the “watering hole,” the attacker pounces.

Once the victim’s device is infected, the user can easily spread the malware to other employees through email, file sharing, or other forms of digital communication over the company network, which

THE PRICE OF RANSOMWARE

Average ransom paid across all businesses globally:

\$170,404

Average ransom paid by retailers:

\$147,811

Source: Sophos

in turn opens more attack surfaces to execute a ransomware attack, says BigCommerce's Holden.

"The sophistication of a ransomware [attack] is usually determined by who the intended target is and the sophistication of their cyber defenses," he adds. "Less-sophisticated attacks tend to be more spray-and-pray style, [and] are driven by botnets."

A botnet attack is a large-scale cyberattack carried out remotely. It downloads malware when connecting with other devices.



While much has changed on the ransomware landscape the past couple of years, one thing that hasn't is where the attacks originate. Russia, China, Iran, and North Korea are the nations that account for about 80% of all attacks, says Aite-Novarica's Schreider.

One reason Russia is a popular home to cybercriminals, Holden notes, is that it is common knowledge the government will turn a blind eye to such activity as long as the cybercrooks confine their attacks to companies outside the country.

Guarding against ransomware attacks requires a great deal of diligence. Best practices include keeping tight control over network access keys and passwords, using strong passwords, preferably passphrases that are uncommon, and not reusing passwords across multiple sites.

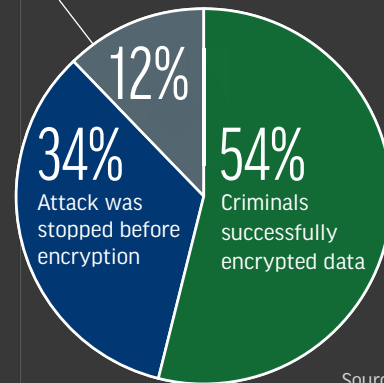
Other strategies include regularly changing passwords and usernames. "Criminals hate seemingly random security changes," says BitMint's Samid. "It requires a lot of work to make those changes regularly, but they can dramatically improve cybersecurity."

The best defenses against ransomware, however, are employee awareness of the problem and a companywide commitment to prioritize cybersecurity daily. "In the majority of cases, the attack vectors would fail if people were aware and prioritized cybersecurity in their day-to-day activities," says Cytelligence's Tobok.

"The majority of [cybersecurity] gaps can be rectified with little to no cost, such as configuring

OUTCOMES OF RANSOMWARE ATTACKS FOR RETAILERS

Data not encrypted, but held for ransom



Source: Sophos

multifactor authentication on cloud email systems, limiting access to externally facing systems, and ensuring backup servers are protected in the event threat actors utilize privileged accounts [to launch an attack]," Tobok continues. "Most of these changes require no additional expenditure except solid processes and some attention."

Still, no matter how strong a retailer's cyber defenses, there is always a risk a cybercriminal will find a way to beat them. So one thing retailers need to keep in mind is that if they choose to pay a ransom, they will become known marks to other hackers, and will likely become the target of later attack from another criminal. As a result, retailers should reassess and revamp their cybersecurity after a ransomware attack, experts say.

"If the business did not learn anything from the attack, did not improve its security posture and close off any security gaps, they are 100% more likely to get hit again and again," says Tobok. "This is precisely why it is critical that any [cyber incident/attack] is investigated properly without cutting any corners. Those who forget history are doomed to repeat it."

With cybersecurity experts forecasting no slowdown in ransomware attacks, and with merchants as a prime target, it's not a question of if a retailer will be attacked, but when. **DT**

HOW TO GET THE MOST OUT OF QR CODES

This new payment technology is spreading fast, but a common set of specifications is urgently needed to ensure global compatibility.

BY **BRIAN BYRNE**

Brian Byrne is director of engagement and operations at EMVCo.

WALK DOWN A STREET in China or India, and it becomes immediately apparent that quick-response (QR) codes are woven into the fabric of everyday life. Nothing demonstrates this more than the boom in QR code-based mobile payments. QR code payment transactions in China have increased 15-fold over the past three years, and 40% of consumers in India regularly use QR codes to make payments.

Even in the United States, where QR codes have been slow to catch on, the technology has enjoyed newfound popularity recently as businesses have sought quick and affordable

ways to meet consumers' appetite for touch-free convenience.

QR codes have provided Americans an easy, hygienic method to view menus and order takeout, redeem coupons and rewards, and return online purchases. This emergence of QR codes across retail and commerce in the U.S. has significant implications for payments.

Payment convenience and choice are increasingly important to consumers. The pandemic has intensified these expectations with more demand for socially distanced options that enable simple, touch-free transactions. A recent study found that 84% of consumers around the world expect to make purchases when they want and how they want. In fact, 60% indicated they have changed shopping behavior in recent months with convenience and value in mind.

Merchants in the U.S. and globally are working to meet evolving consumer demands by supporting a range of consistent and convenient payment methods. As a relatively low-cost option requiring minimal equipment and setup, QR codes have attracted businesses aiming to pivot quickly in the midst of a pandemic and beyond.



A SINGLE TERMINAL

The potential is huge. Juniper Research indicates that the ability of QR codes to combine payments and loyalty makes them ideal for retailers seeking to leverage valuable transactional data. It predicts that the low-cost nature of these solutions will enable the value of QR code payments to grow to more than \$2.7 trillion globally in 2025. In the U.S. alone, the number of QR code payments is forecast to increase 240% by 2025.

Realizing this potential, however, is anything but guaranteed. A consistent, reliable, and easy consumer experience is key to any payment method thriving, and it is no different for QR codes. As the trend towards contactless options continues, whether it is tap-to-mobile or QR code, consumers will gravitate to businesses and providers that make it simple for them to pay how they want.

Solutions that support multiple and new payment options efficiently and seamlessly to deliver a frictionless consumer-centric experience will drive adoption forward.

In contrast, fragmented ecosystems with various incompatible solutions create user confusion and frustration, as was the case in the early days of card acceptance when it was common in many parts of the world for merchants to have multiple terminals at the point of sale. The consumer or the merchant had to figure out which terminal was appropriate for a specific transaction.

As happened with chip terminals, the most efficient and consumer-friendly solution is a single terminal capable of supporting multiple



“Creating common technical foundations for QR code-based payments is critical.”

payment options. It would introduce unnecessary friction to have multiple QR codes at the point of sale when one QR code is capable of supporting all payment types. For this reason, creating common technical foundations for QR code-based payments is critical.

COMMON BUT FLEXIBLE

EMV Specifications provide a baseline of technical requirements that enable any party to develop payment products and solutions safe in the knowledge that they will work together seamlessly anywhere they are used to deliver consistent and convenient payments. Consumers and businesses benefit from the EMV Specifications every day by being able to follow a familiar payment process to make secure, reliable, card-based payments wherever they are in the world.

Key to the success of EMV Specifications is that they are global, meaning any business in any country can adopt them and expect their solutions to work everywhere. Just think about the EMV Chip Specifications. Prior to their development, France was building out specifications to support secure chip payments and the U.K. was doing the same, but the two were not interoperable.

EMVCo was formed so everyone could use the same specifications, and they would all work together. Now, EMV chip transactions are

near-ubiquitous in the U.S., and are used around the world (close to 90% of card-present transactions globally are EMV chip-based).

Importantly, the flexibility of EMV Specifications means that this global interoperability does not come at the expense of meeting local requirements. For example, the U.S. was able to adapt the global EMV Chip Specifications to support the industry's need for a Common Debit AID (Application Identifier) on EMV chip cards to provide merchants debit-routing options in accordance with U.S. regulation.

The EMV QR code Specifications provide a standardized template for the generation of QR codes for payments. This means QR codes will work in the same way, no matter where they are used for the delivery of quick, reliable, and trusted transactions for both merchants and consumers.

At the same time, where QR codes have the potential to unlock opportunities for new use cases and future advancements for a specific industry sector or region (such as the basis for instant payment initiatives and e-invoicing remittances, or next-generation loyalty and rewards offerings), EMV QR Code Specifications provide the flexibility to support innovation and additional features and functionality, while still providing consistency and interoperability across solutions and geographies.

This flexibility is made possible through engagement with payments stakeholders from across the world who provide input into the development of EMV Specifications and vote on whether they are ready for publication.

COMMON FOUNDATIONS

For these reasons, countries around the world—from India to South Africa to Colombia—are already using or considering implementing EMV QR Code Specifications. In Europe, the European Payments Council has advised that “existing QR code-based solutions should consider migrating to the

EMVCo specifications to enhance the interoperability of their solutions.”

In Canada, Ernst & Young is working with industry stakeholders on QR code payment adoption and using EMV QR code specifications in its efforts to “harmonize [QR code payments] across market participants from coast to coast.”

As U.S. consumers continue to prioritize choice and convenience at the point of sale, and businesses look for reliable, and efficient ways to accept QR code payments, EMV Specifications offer a common foundation for QR code payment solutions. These solutions will work both domestically and inter-

nationally, support multiple payment options, and enable merchants to increase consumer engagement with loyalty and reward programs—all using just a single QR code at checkout.

This means that, when at home or abroad, consumers can expect a frictionless QR code payment experience that is consistent, familiar, and easy, and that supports their shopping preferences.

While QR code payments are still gaining traction in the U.S., we can expect continued acceleration. Laying common foundations now will prevent challenges down the line. **DT**



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.omedacom/dtr/
or email publisher Bob Jenisch at Bob@digitaltransactions.net

Time for banks to
flip the script.

FIXING OPEN BANKING'S ONE-WAY STREET

Financial institutions have been cooperating with fintechs for years on data exchanges. But now banks need to get on the receiving end, says Sarah Grotta.

BY SARAH GROTTA

Sarah Grotta is director of the Debit and Alternative Products Practice at Mercator Advisory Group, Maynard, Mass. Reach her at sgrotta@meractoradvisorygroup.com



CONCEPTUALLY, OPEN BANKING is a straightforward premise. Consumers allow their financial institution to share specific financial data electronically and securely with authorized third parties. Access to data is completely controlled by the accountholder and can be changed at any time.

The financial-services market is excited about the opportunity presented by open banking, given the multitude of use cases it can empower.

Popular use cases that can bring better financial outcomes for end users include sharing checking-account and routing numbers for inclusion in a payment wallet, gathering balance and transaction data for a third-party savings and budgeting application, and including financial information that could help make credit decisions when applicants have little or no formal credit reporting.

The United States is being ridiculed in the global payments industry (yes, again) for not having a top-down, regulated, and mandated approach to open banking as they do in the United Kingdom, the European Union, and Australia. In these countries, specific data sets must be shared upon request through standardized application programming interfaces with third parties that are vetted by regulatory agencies.

U.S. financial institutions are generally not opposed to the idea of open banking, but they are wary of how a mandated approach may put them in the position of having to bear all the responsibility while enjoying few benefits. A minefield of unanswered questions exists:

- ▶ Who bears a loss when unauthorized data finds its way into the hands of criminals?
- ▶ Who manages a consumer's changing preferences for which data points they allow to be shared?
- ▶ What is owed to the consumer whose data is shared in error, violating privacy rights?
- ▶ What are the appropriate authentication tools to have in place?

Besides these perils, any one of which could put a financial institution in regulatory hot water, there are simple, functional rules-of-the-road questions that must be addressed:

- ▶ Whose data standards should be used?
- ▶ Who will manage API development and how?
- ▶ Should requesters expect to pay for the data they receive?

Financial institutions that have already lost so many accounts and

transactions, not to mention the loyalty of their customers, to fintechs believe open banking is just one more way that non-financial companies, unburdened by the regulatory oversight and profitability requirements banks bear, will siphon off even more account relationships.

While I would be shocked if a mandate for open banking were issued in the U.S., regulators will be shaping the rules of play. The Consumer Financial Protection Bureau issued an Advance Notice of Proposed Rulemaking (ANPR) in 2020 titled “Consumer Access to Financial Records,” and asked for industry participation to better understand which data points should have protected access, how security of data should be managed, how to ensure appropriate data privacy, how to provide consumers the ability to control what data is shared, when and with whom, plus who bears responsibility for unauthorized access to data as well as data errors.

These are very weighty subjects that could use well-thought-out

guardrails that don’t stifle innovation.

Here’s the funny thing. Despite the Wild West environment of open banking, it’s already in place in the U.S. and being used by millions of households. Banks and credit unions have established bilateral contractual agreements with the data aggregators that want access to account data to legally lock down the unanswered questions.

While this may appear to be an imperfect approach that is hard to scale, it seems to be working. Plaid, just one example of an aggregator of consumer financial data, reports having processed data for 98 million individuals from the U.S.

So, without a government mandate, open banking is alive and functioning and expanding rapidly based on market-driven needs. Those who want to keep it at bay are fighting a losing battle.

IT’S A FINTECH WORLD

In these early days of U.S. open banking, fintechs are pounding the table,

demanding that “something be done” so that they may have the right to access account holders’ information uniformly across all financial institutions, with promises for better financial-services products at better prices. What isn’t being heard is financial institutions requiring the same of fintechs— and that’s a missed opportunity.

Banks should flip the story around open banking. They should ensure that this is not just a one-way proposition where fintechs and big tech are requesting all the important data while more-traditional financial institutions are doing all the giving.

This presents some interesting opportunities. Consider the following scenarios:

- ▶ A financial institution pulls in permissioned data from PayPal, Venmo, and Cash App to provide a more holistic view of a consumer’s available balance across accounts. The financial institution could then advise the account holder that they should pull in funds from another source to avoid an overdraft.
- ▶ A financial institution may query a consumer’s buy-now-pay-later apps or existing credit card accounts and offer a better alternative.
- ▶ Or if small-business data is included in open banking, fee data from a business’s merchant statement for services they are receiving from a fintech, or another financial institution for that matter, could be analyzed, and an alternative product offered.

These are all ideas that fintechs are already considering. Banks should be doing likewise. DT

ADVERTISER INDEX

Digital Transactions Page 19, 30
877-658-0418 www.digitaltransactions.net

Electronic Merchant Systems Back Cover
866-596-8829 www.emsagent.com

eProcessing Network Page 9
800-296-4810 www.eprocessingnetwork.com

First American by deluxe Page 15
866-464-3277 www.first-american.net

General Credit Forms Inside Front Cover
888-GCF-News www.gcfinc.com

Magtek Page 3
562-546-6400 www.magtek.com

Merrick Bank Merchant Acquiring Page 17
844-320-7100 www.merrickbankacquiring.com

Northeast Acquirers Association Page 25
www.northeastacquirers.com

Round 2 POS Page 5
800-283-9037 www.round2pos.com

Shift4 Page 1
800-201-0461 www.shift4resellers.com

Wholesale Payments Page 21
806-686-1717 www.wholesalepayments.com



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



emsagent.com | 866-525-7405

What's in your hand?

Don't lose another deal! Partner with the industry's best Agent Program today.

