DIGITAL TRANSACTIONS

Trends in the Electronic Exchange of Value

SHOULD CBDCs BE THE NEXT BIG THING?

The risks may outweigh the benefits

Volume Nineteen, Number Two • DigitalTransactions.net • February 2022

ALSO IN THIS ISSUE:

Cashing in on Cash

The A2A Grand Prix

E-Commerce's Momentum

Thwarting ACH Fraud

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 *Digital Transactions* magazine

Detailed listings of payments market suppliers

13 years of payments news and analysis

DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

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

contents

FEBRUARY 2022 • VOLUME 19, NUMBER 2

Should CBDCs Be the Next Big Thing? 20

The answer may be more complicated than you think.

THE GIMLET EYE Amazon, Visa, And the Rate Wars 4

TRENDS & TACTICS 6

How Processors Can Cash in on Cash

Brink's is courting ISOs to help sell merchants on a digital overlay for notes and coins.

The Risk of Too Much BNPL

The credit option is wildly popular—and may lead some to miss payments.

Who Won the Pandemic Payments Sweepstakes?

If you guessed the ACH, you're right.

Chuck Isn't David, But It's up Against Some Goliaths

Why should merchants and card issuers have all the fun?

Plus, Security Notes explains the allure of self-referential money; and Payments 3.0 outlines how the regulatory climate is getting a little uncomfortable for payments.

ACQUIRING 13

The Crutial Race for Account-to-Account Payments

The market for direct transfers between bank accounts is attracting fintechs—as well as the two global card networks—as real-time payments loom.

E-COMMERCE 16

Why the E-commerce Meteor Will Burn Bright Post-Pandemic

Consumers have turned to mobile and desktop buying in record numbers. Merchants and processors are figuring out how to sustain the surge.

SECURITY 28

Top Tips for Preventing ACH Credit Fraud

It's become more common and harder to detect. Here are some measures that can help cut it down to size.

ENDPOINT 31

When Fraudsters Take a Vacation

Theft of loyalty points has become a serious issue in the travel industry. But is it being taken seriously by hotels and airlines?

Cover Illustration: Jason Smith, 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.

MAGTEK®
SECURITY FROM THE INSIDE

Bringing what you love together with how you pay

mobile payments with contactless and touchfree technology

iDynamo 6

Merchants will benefit from iDynamo 6, the next generation of MagTek mobile secure card reader authenticators (SCRAs).
MSR | EMV | NFC

MPPG

Magensa Payment Protection Gateway is our payment gateway supporting traditional Sale, Auth, Capture, Void, and Refund transactions to integrated processor endpoints.

Development

MagTek is your partner in development and provides a comprehensive platform for drivers, APIs, and SDKs to speed your efforts and get to market faster.

Scan to view iDynamo 6 videos

FIND OUT MORE

562.546.6400
sales@magtek.com
www.magtek.com

MagTek, Inc., 1710 Apollo Court, Seal Beach, CA 90740

the gimlet eye

AMAZON, VISA, AND THE RATE WARS

WILL THE CONFLICT BETWEEN MERCHANTS and the card networks over acceptance fees ever find resolution? The argument, which has been in progress for years, may never find total resolution, but perhaps the parties can agree on some accommodations.

Amazon.com Inc.'s decision last month to pull back from its threat to stop accepting Visa cards issued in the United Kingdom may indicate some flexibility on both sides. The move certainly betokens some complex dynamics behind the decision-making at both corporate giants as rate revisions loom.

Amazon backed off on a Visa ban it announced in November as part of a protest against acceptance fees. The massive online merchant said then it would stop taking Visa in the U.K beginning Jan. 19. But in a terse email message it sent to customers on the eve of the ban, Amazon hinted that negotiations may yield a new agreement.

While some observers may have been tempted to conclude Amazon blinked in the face of losing Visa's considerable heft in the U.K. market, others say the move likely comes as the culmination of long weeks of strategizing on both sides. Certainly, Amazon's had to consider the impact of losing some portion of the billions of pounds Visa accounts for on Amazon's site in the U.K.

But pressure was on Visa, as well, especially as it faced the prospect of consumers switching to other cards as they shopped on Amazon. Some observers say this fact alone may have brought the network giant to the table.

Certainly, if Amazon's aim in all of this was to get Visa's attention and to start negotiations, that has been accomplished. Now the payments industry is likely to watch the talks closely, given what's at stake. And some observers argue Amazon's leverage is likely to prevail. Visa's fear of seeing Amazon sales flowing to other card brands, they say, could be greater than Amazon's nervousness that some sales will be lost altogether.

After all, Amazon may enjoy added leverage in its talks with Visa as a result of its willingness to accept widely used alternative payments, most recently PayPal Holdings Inc.'s Venmo wallet, some observers point out.

These intricate negotiations come as Visa and Mastercard are preparing to roll out new rates this spring. They had intended to introduce a variety of increases, with some reductions, last year but held off in view of the pandemic and its impact on many merchant categories. They aren't likely to postpone the changes again.

That's food for thought for most merchants—particularly those that, unlike Amazon, lack the huge sales volumes and market share that can get the attention of nervous networks.

John Stewart, Editor | john@digitaltransactions.net

FEBRUARY 2022 • VOL. 19, NO. 2

DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

PUBLISHER Robert A. Jenisch

EDITOR-IN-CHIEF John Stewart

SENIOR EDITOR, DIGITAL
Kevin Woodward

CORRESPONDENTS
Jim Daly, Peter Lucas

ART DIRECTOR/PRODUCTION EDITOR
Jason Smith, 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.

BPA WORLDWIDE

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

HOW PROCESSORS CAN CASH IN ON CASH

Lost in much of the conversation about digital payments, particularly since the onset of the pandemic, is what to do about the cash merchants take in. The Brink's Co., which has been hauling and securing cash since 1859, says it has an answer, and in January it announced it also has an agreement with a major payments processor to bring that solution to merchants.

Priority Technology Holdings Inc. has agreed to participate in BLUbeem, a program Brink's announced in December to let merchants take in cash payments and have them credited through a mobile app to their bank accounts through Brink's. Alpharetta, Ga.-based Priority will sell the service alongside its processing of credit and debit card payments, the companies said. Priority says it serves 250,000 merchants through ISOs and independent software vendors.

Some 20% to 25% of the payments taken in by the merchants in Priority's portfolio occur in cash, the company adds, pointing to a sizable opportunity to resell BLUbeem.

"Expanding our reach into cash payments will allow Priority to introduce a variety of new solutions into the market, helping improve customer retention and driving growth into new channels," said Tom Priore, Priority's chairman and chief executive, in a statement.

With BLUbeem, merchants store their day's cash receipts in a bag supplied by Richmond, Va.-based Brink's, then place the bag into a small safe-like device also supplied by Brink's.

Brinks: How to process cash digitally

They enter the cash total in the app, with Brink's crediting the funds to the merchant's bank account. Brink's then arrives later to pick up the cash and take it to the merchant's bank. This method, Brink's says, allows cash intake to settle as fast as credit and debit card payments.

The market size could be considerable. Brink's estimates some 1.6 million U.S. merchant locations lack what it regards as an "effective solution" for cash payments.

Similar services are available from other cash-transport companies, but these typically restrict deposits to a specific bank, according to Josh Allen, vice president of digital payments at Brink's. "They're not bank-agnostic" like BLUbeem, he says. Fees for each deposit typically fall into the 1% to 3% range, he adds, alongside what he calls a "small upfront monthly fee" to lease the safe-like cash-storage device.

Brink's clearly has big ambitions for the new service. In its December announcement of BLUbeem, the company said its strategy is to integrate the service into merchants' existing point-of-sale systems, requiring ties with ISOs and other payments providers.

"We have a tremendous white-space market opportunity," Rohan Pal, chief digital officer at Brinks, said in a statement at the time. "By creating commercial partnerships with digital payment companies, we can leverage their sales channels to reach these merchants."

In addition to Priority, Brink's has so far forged a partnership with FIS Inc. for BLUbeem, Allen says, adding there are other arrangements not yet named.

—John Stewart

THE RISK OF TOO MUCH BNPL

Buy now, pay later loans are extremely popular, especially among Millennials and Gen Zers, because they give users more purchasing power, and they can spread out the payments, usually without having to pay interest.

Yet, despite the immense popularity of BNPL loans, evidence is emerging that consumers with multiple such loans open at any time are likely to miss a payment. A January survey of some 1,500 BNPL users by Breeze, a provider of disability insurance that follows personal-finance trends, revealed that 48% of users with multiple BNPL accounts open have missed a payment. Concerns over the rate of BNPL delinquencies began to emerge last year.

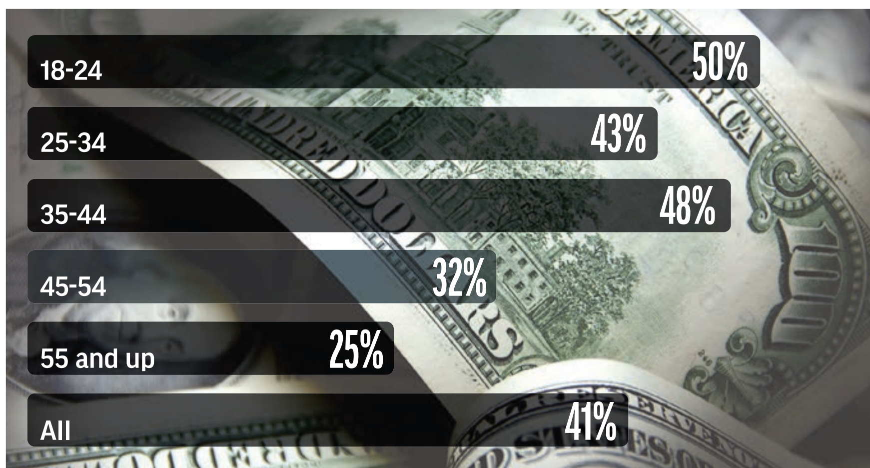
"That nearly half of BNPL users with multiple accounts have missed a payment is surprising, considering the average ticket is not all that high and no interest is charged," says Mike Brown, director of communications for Breeze, the trade name for Hoboken, N.J.-based Modern Insurance Agency Inc.

Overall, 36% of respondents say they have missed a BNPL payment at least once, a figure that Brown also found on the high side. One culprit for the delinquency rate could be that BNPL lenders tend not to perform extensive credit checks, if any at all, when qualifying applicants, observers say. As a result, BNPL lenders may have opened the door to qualifying consumers with poor credit ratings who may be overextending themselves with too many BNPL accounts.

While 41% of BNPL users said they have had multiple BNPL accounts open at one time, 57% of users said BNPL has caused them to spend above their means. A tendency to overspend with BNPL has a direct correlation to missed payments, according to the study.

CAN'T JUST STOP AT ONE

(Percentage of BNPL users who have had multiple accounts open at the same time, by age)



Source: Breeze survey of 1,500 adult consumers in January

"When a consumer has multiple BNPL accounts open, even though the payment for each account may be manageable by itself, paying on multiple accounts at once can snowball on a consumer and lead to missed payments," says Brown. "This is something to keep an eye on going forward."

Signs that credit overreach is emerging is likely to bring increased scrutiny from regulators, Brown says. Last month, the Consumer Financial Protection Bureau (CFPB) issued a letter to five BNPL lenders demanding data about their respective operations. Shortly afterward, Equifax Inc. announced it would become the first credit bureau to add BNPL data to consumer credit reports, a move that is expected to help BNPL lenders manage their risk better.

"Recent reports have suggested Capitol Hill, the credit companies, and the CFPB will all start looking at the BNPL industry with more scrutiny," says Brown. "Most BNPL companies right now are not really looking intently at credit usage or history during the application process and it's possibly leading to BNPL distributing too much unwarranted credit."

A primary reason consumers apply for BNPL loans is that many have poor credit histories. Of the BNPL users surveyed, 45% said they started using BNPL because of a bad credit rating. As a result, the popularity of BNPL loans is starting to rival that of credit cards. Indeed, 63% of BNPL users believe BNPL is a better product for financing purchases compared to a credit card and 61% say BNPL has reduced their credit card usage.

"BNPL is becoming a competitive threat to credit cards, especially among Millennials and Gen Zers, because they don't like the idea of paying off high-interest-rate credit card debt," Brown says. "BNPL also is a way for people to make purchases without depleting their savings and is one of the trendiest personal finance products at the moment."

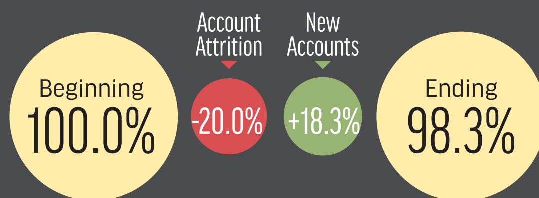
—*Peter Lucas*

MONTHLY MERCHANT METRIC

Oct 2021 Account Attrition and Growth

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

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



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

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

WHO WON THE PANDEMIC SWEEPSTAKES?

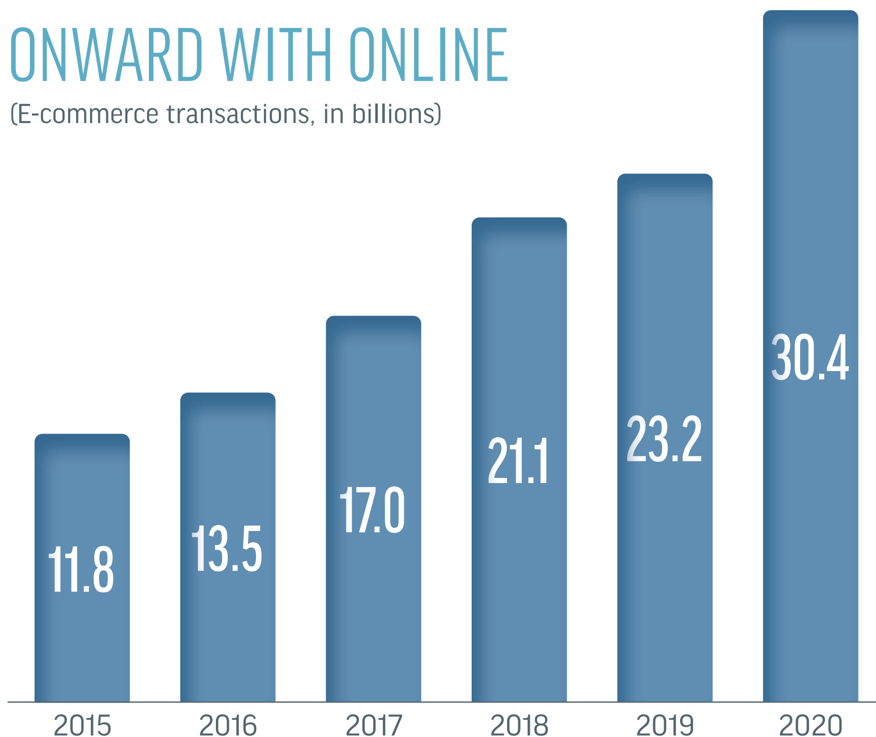
The share of payments claimed by the automated clearing house rose faster in 2020 than the shares for cards, while checks dropped markedly. All the while, the share of payments claimed by cards, which had been steadily on the rise for years, flattened out. And while contactless transactions did rise fast, they still account for a very small share of all card payments.

All of this is according to the latest payments data released in December by the Federal Reserve Payments Study.

The data, which the Fed gathered quarterly in 2020 for the first time, show a surging ACH, with the Fed estimates indicating the massive, 47-year-old network was the only payment system to increase in 2020 by number of transactions. In part, this came about as the pandemic drove down in-person card transactions, offsetting increases in online activity, the study indicates.

Looking at the three primary payment systems—cards, checks, and ACH—card transactions as a share of all transactions dropped slightly in 2020, to 74.25%, according to the data. ACH, on the other hand, saw its share climb to 19.24% from 17.87% in 2019. Checks declined to 6.51% from 7.5%, continuing a long-term trend.

The drop in cards' share, though just 0.39 percentage point, was nonetheless significant, the study says, as it represents the first such decline detected by the Fed since it started making estimates nearly 22 years ago.



Helping to drive the rise in ACH's share were a number of factors, according to the study, including more payments by both consumers and businesses as well as increasing use of the ACH for settlement of small-value transactions, including those done through mobile devices. At the same time, such traditional transfers as bill payments and payroll deposits grew in number "at a faster rate than in previous years," according to the study.

As for cards, the pandemic "ushered in an unprecedented shift from in-person to remote card payments," the study says. In-person payments dropped by 11.7 billion in 2020, the first decline of any amount in this category seen by the series of Fed studies. Remote transactions—which include e-commerce—grew by 8.7 billion, the biggest such one-year rise observed by the Fed but not enough to offset the plunge in in-person activity.

At the same time, the number of contactless card payments soared fully 172% in 2020 over 2019, reaching 3.7 billion. This performance followed an already impressive rise of 121% in 2019 over 2018. The big increase in 2020 left contactless at 4.63% of all in-person card payments, according to the study, up from 1.7% in 2019 and 0.77% in 2018. As impressive as that is, however, the study cautions that 4% remains a relatively small number.

Payments from digital wallets also enjoyed a boost in 2020, accounting for 2.6% of all credit and non-prepaid card transactions. That was up from 0.50% in 2017, but the rate of increase was much faster in 2020, suggesting, the study says, that "the pandemic may have resulted in account holders making more digital wallet payments than they would have otherwise."

—John Stewart

CHUCK ISN'T DAVID, BUT IT'S UP AGAINST SOME GOLIATHS

Rather than compete directly with Zelle and other big peer-to-peer payment networks, the recently launched Chuck network plans to position itself as a P2P network that eases money transfers for users, officials say.

One such feature in the works is the ability for users to create a directory of destinations to allow faster transactions when money is sent to specific individuals. For example, if John Smith typically sends money to Jane Doe's crypto wallet, that information can be stored and automatically invoked to send future payments to Jane Doe, according to Jason Henrichs, chief executive of Alloy Labs Alliance, a consortium of community and mid-size banks backing Chuck.

"We want consumers to be able to send money where they want, and if someone prefers to receive money in their bank account or in a social-media account, money can be sent there," Henrichs says. "This is about creating a better user experience, not competing with Zelle."

Ten community banks launched the Chuck network in December as an alternative P2P system. The new network uses technology from digital-payments platform provider Payrailz LLC that enables customers of any of the member banks to send money to a debit card or bank account outside the Chuck system, as well as within it. The 10 founding members are part of the Alloy Labs Alliance.

Creating strong brand recognition will likely be key to the network's success, says Sarah Grotta, director of the debit and alternative products advisory service at Mercator Advisory Group.

"Banks coalesced around Zelle because they thought it was important to have a single brand for P2P payments," Grotta says. "That's where prior P2P networks failed. It will be interesting to see how consumers respond to this."

Henrichs counters that a single brand for the new P2P service is not imperative, as member banks will be marketing the service using their brand. That strategy is logical, he says, as members have embedded the service in their respective mobile-banking apps, which they brand themselves. Chuck is the name for the network behind the P2P service.

"Popmoney had a single brand and never took hold," Henrich says. "Banks can brand [the service] however they want, but because it is part of their mobile-banking apps, it is part of the banks' [branded services], not another P2P app consumers have to download." Henrichs says. "Banks can also layer on other features through the mobile app to enhance the user experience. We think the people this will appeal to are those that have not downloaded a P2P app."

One advantage Chuck offers to community banks will be a lower fee structure than that of Zelle, which reportedly charges participating banks between 50 cents and 75 cents per transaction. Alloy Labs plans to set fees based on a bank's size and transaction volume through the network.

"A bank of modest size probably isn't going to generate the volume that earns them the lowest price." Henricks says. "Our approach is to offer a reasonable price based on the bank's size and volume."

Lower transaction fees are expected to play well with community banks looking to add a P2P service. "Smaller banks have struggled with Zelle because of the fees," Grotta says. "And if they connect to Zelle through a processor, the processor layers on its own fees, which raises the costs further."

The ability to provide advanced digital payment services to consumers is important for small banks, as 60% to 70% of consumers use P2P apps, Grotta says. "If small banks want to be thought of as the place to go for digital services, they need these kinds of capabilities," she adds.

—Peter Lucas

THE LURE OF SELF-REFERENTIAL MONEY IN A CRYPTOCURRENCY AGE

BY GIDEON SAMID
gideon@bitmint.com

IN RETROSPECT, BITCOIN had to be expected. Secular humanism challenges God-centered culture, and quantum physics redefines reality to what we humans measure—nothing more. So money that is hinged on nothing external to itself is a natural followup. But if this self-anchored philosophy is wrong-footed, then as it rises to dominate the global exchange of value, it becomes a ticking time bomb. That give us much to worry about.

The Financial Times in a recent article declared that Bitcoin is worse than a Madoff-style Ponzi scheme. Quite a few highly credentialed observers agree, but reality laughs in their face. Self-referential money led by Bitcoin has entered triumphantly into its second decade, and every day more skeptics plunge in. The arguments in favor of Bitcoin being a gigantic, long-lasting Ponzi scheme are solid. But if the "Big Bang" was created from nothing, and the universe simply runs on its inertia, why can't money do the same?

Theoreticians are working on it. The most promising idea to establish a firm foundation for self-referential money like Bitcoin is to add to the protocol a price-stability tax. The death scenario for Bitcoin is as follows: afraid of missing out, more and more speculators buy the currency; the price goes up and dissolves the hesitancy of those holding back; and a mad feedback cycle gets the price into ridiculous heights until it flips, dropping into a free fall. It turns out that the Bitcoin protocol can be tweaked to prevent this "death scenario." The network will designate a threshold price for the coin, and will prevent the coin from exceeding this threshold by dumping enough coins into the market to tamp down the price.

But where will these coins come from? From the network acting as a "government," taxing the coinholders. One peculiar feature of Bitcoin is the fact that all outstanding coins are exposed to the public. Their owners hide in the complexities of the mathematics, but the coins themselves are completely visible. It is therefore possible for the protocol to chip a cut from each coin, say 1.5% of its value, and siphon these "chips" to a Price Stability Fund, from which they would be dumped in sufficient quantity to prevent the price from exceeding a preset threshold.

Ideally, the coin will have a fund of its own money and a fund of the money it is priced for, say the U.S. dollar. However, there is no theoretical way to manage a dollar fund through an automated protocol, so this stability tax, being protocol-limited, is only possible one way: to prevent an out-of-bounds price hike.

When the price of the coin inches toward the preset intervention value, speculators will lose interest and drop out. The currency is then left for traders to treat it as money *per se*. The longer the period of time this coin stays stable—close to the designated threshold—the more inertia develops, confidence builds up, and the currency looks like money, not like a get-rich-quick scheme.

The designated threshold must be voted on by the traders. And, since anyone can open as many accounts as he wishes, the only fair way to allocate voting power is by ownership of the currency. Alas, Bitcoin, as an example, is a currency with an extreme concentration of owners: 0.01% of traders own about one-third of the currency. What the currency is worth will be their call.

If history is any guide, the essential innovation inherent in self-referential currency will be recast as a digital currency hinged on human assets that have a presence outside the trading protocol. DT

A LESS COZY REGULATORY CLIMATE

BY BEN JACKSON

bjackson@ipa.org

THE CONSUMER FINANCIAL PROTECTION BUREAU'S recent data requests show how regulators are teaming up and provide clues about the near future.

In October 2020, the Bureau announced that it requested data from Amazon, Apple, Facebook, Google, PayPal, and Square (now Block) about their payments operations, and that it would compare what it learned with research into Chinese fintechs Alipay and WeChat Pay. They asked about data harvesting and monetization, the notion of locking consumers into using their products, and consumer protection.

Then, in December, the Bureau sent detailed data requests to buy now, pay later companies Affirm, AfterPay, Klarna, PayPal, and Zip. In a 16-page request, it asked for detailed information about these companies' operations, customer bases, and revenue models. It also included specific questions about data harvesting and monetization.

The in-depth questions about data harvesting and monetization in both requests show that data and privacy will become important issues. Depending on what the CFPB finds, we may see a round of regulations that focus on data and its use.

But the questions about whether customers are locked into using particular platforms show a bigger picture. Regulators are increasingly concerned about the size of companies. For example, the Federal Trade Commission has sued Facebook, asking a judge to order it to sell WhatsApp and Instagram.

As all of this is happening, the Bureau's director, Rohit Chopra, who sits on the board of the Federal Deposit Insurance Corp., has, along with Martin Gruenberg and acting comptroller of the currency Michael Hsu, forced the FDIC to issue a request for information about the Bank Merger Act. One of the questions is whether any transaction over a certain size should be considered a systemic risk.

The request—first published on the Bureau's site and not the FDIC's—led to a battle over whether the Board could do this without the cooperation of FDIC chairwoman Jelena McWilliams, who then announced she will resign in February.

These changes suggest that the banking regulatory agencies will be working more closely with one another in the future. It is not likely that the next head of the FDIC will be able to avoid going along with the other regulators.

Meanwhile, the CFPB is still locked in a court battle with PayPal over the disclosure requirements of the Bureau's prepaid accounts rule. If the Bureau loses, it may take that as a catalyst to write new regulations that would address the gaps left by the lawsuit.

While the information that comes out of the data requests will not likely influence the ongoing cases, they show that certain topics have regulators' attention across industries.

The payments industry will need to keep its eyes open for regulatory action on a variety of fronts. It will also need to pay attention to whether state and federal regulators are working in concert.

The industry needs to keep two things in mind.

First, the regulators do not care about whether your businesses thrive or even survive. In their minds, that is secondary to whether any consumer harm happens at all. If 100 people benefit, but one misuses a product, that is often enough to ban it.

Second, the industry needs to tell its story in a coordinated way. While companies may see a temporary competitive advantage in some regulations, if only one company or business model is left, then that will be the one that gets all the future scrutiny. As regards point one above, eventually regulators will come for the last one standing.

Relationships with regulators are about to become more intense. Companies should be working on strategies for weathering the new climate. DT

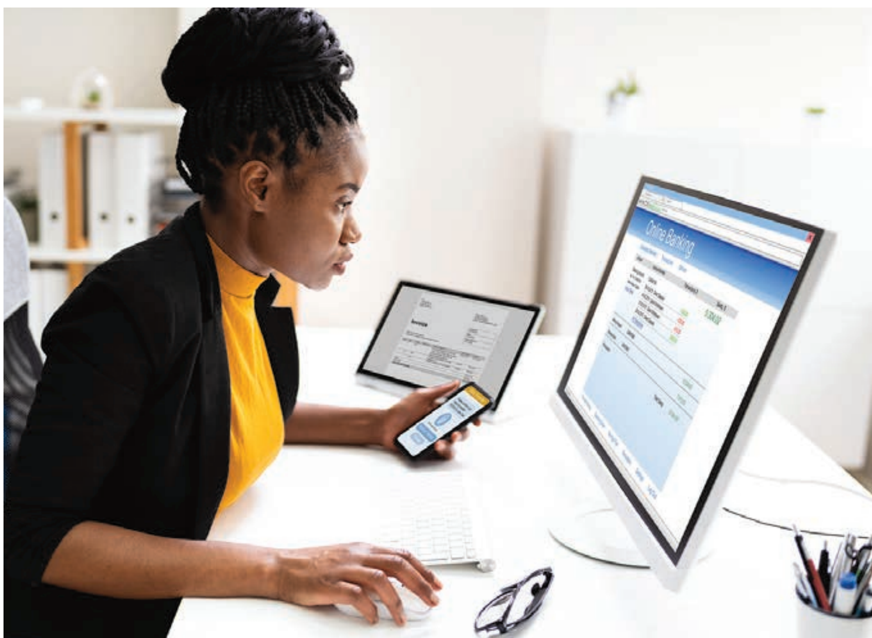
THE CRUCIAL RACE FOR ACCOUNT-TO-ACCOUNT PAYMENTS

The market for direct transfers between bank accounts is attracting fintechs—as well as the two global card networks—as real-time payments loom.

BY KEVIN WOODWARD

WHILE ACCOUNT-TO-ACCOUNT TRANSACTIONS—think the automated clearing house—have been around for years, the shift to real-time payments is giving them a new boost.

Little happens overnight in the payments industry. While account-to-account payments appear to be building momentum quite quickly, the concept has been implemented in reality for some time. Consider ACH transactions. The first ACH association formed in 1972 and today, as of the 2021 third quarter, the ACH network had 7.3 billion transactions, all flowing from one account to another.



Broader forms of account-to-account transactions now are surfacing, capturing the attention of fintechs, payment providers, and the card brands. Questions abound, including which use cases stand the best chance of success, what is the growth potential, and how to develop a large market for A2A transactions.

"Let's start with what merchants want to get done," says Siamac Rezaiezadeh, director of product marketing at GoCardless Ltd., a London-based specialist in account-to-account transfers. Sellers want payment methods that convert well, have high success rates, and enable them to get their money quickly, Rezaiezadeh says. "And they want the transaction to be highly visible and secure and have low cost."

Buy now, pay later provider Klarna AB recently enlisted GoCardless to enable direct transfer from a bank account. Consumers typically use a debit card to fund their BNPL purchases.

Rezaiezadeh generally classifies account-to-account transactions as push and pull types. Pull is like an ACH debit, such as when a biller withdraws funds from a bank account to pay a utility bill. The push type is more dependent on the payer moving the money transfer.

One appeal of account-to-account transactions is they can yield high success rates. For example, one area where A2A transactions might fit well is recurring payments, Rezaiezadeh says.

"A lot of merchants today have moved to a recurring-revenue business model, like subscription or card-on-file," he says. These transactions may generate as much as a 10% failure rate because of various factors, such as insufficient funds, an expired card, or the issuer blocked the transaction. (Capital One Financial Corp. began in 2020 blocking buy now, pay later transactions made with its credit cards, but permits them with debit cards.) "When moving to billing the account directly, you have a lower failure rate, like 2.5%."

CONSUMER CHOICE

Though it might seem incongruous, card behemoth Visa Inc. sees opportunities for it in account-to-account transactions, especially when powered by the speediness of real-time payments. Many account-to-account transactions have been processed as a batch at the end of the day or similar period. Adoption of real-time payments means these payments can process as they happen.

"As more countries move to real-time payments, it makes account-to-account a little more usable," says Mark Nelsen, Visa senior vice president of open banking. "One challenge with legacy account-to-account transactions, because it was batched, there was a chance with batched there may not be funds available when processed."

Best known for its card payments—Visa's U.S. card transactions tallied 21.9 billion in the 2021 third quarter—the card brand has taken notable steps to strengthen its position in account-to-account payments. In 2021 it announced Visa Direct Payouts, which enables users to send funds to either a recipient's Visa debit or prepaid card or to his or her bank account. The transfers can be made to more than 170 countries.

It has also long offered Visa Direct, which enables real-time or near real-time transactions between Visa card accounts. And its competitor, Mastercard Inc., continues to build its foundations for account-to-account transfers.

"We see [A2A] as an opportunity, a way to get volumes we've not historically been involved with," Michael Miebach, Mastercard chief executive, said in October. Addressing an analyst question then, Miebach denied the race to build A2A capability will hurt his company's core card business. "We don't see a disintermediation risk. I see a way to form partnerships and improve our [transaction] flows," he said. "It's still early days."

Similarly, Nelsen dispels the notion that account-to-account transactions will harm Visa's core business, though he acknowledges there may be use cases where the payment method is a better fit than a card. That's why Visa is involved now, in the early days, he says.

The example he cites is when an individual has a $10,000 tax bill to pay, but the person's bank may have a daily debit ceiling limit. There are two possible ways to accommodate this situation. One is to enable account-to-account transactions. The other is to make card-based payment as seamless as possible, Nelsen says. "Ultimately, Visa wants to give consumers choice," he says.

'VERY OPTIMISTIC'

And there is inertia to contend with. Consumer payment behavior is well known for being difficult to change absent something like a pandemic—contactless payments finally took off in 2020 after 15 years—and a large migration from cards to account-to-account transactions, overall, is expected to take time. Consumers

The GoCardless app: On its way to a global network?

may not even realize they completed an account-to-account transaction at times, Nelsen says.

Consumers, too, have grown accustomed to card-based benefits, such as fraud protection and the separation of their own funds from the card's credit limit. In scenarios where the consumer trusts the merchant, there could be some change, he says. "It's hard to get consumers to change something if it's working really well," says Nelsen. "There's always going to be competition. We're going to make sure the card payment process is as seamless as possible."

Consumer willingness to use account-to-account transactions already may be developing. "What's interesting is that we're seeing an overall shift in the mindset and actions of consumers toward payment methods in the last few years," Rezaiezadeh says.

A 2021 survey from GoCardless found that 76% of respondents would like to decrease use of credit cards. Debit cards and no-interest installment payments found a lot of favor. In the 18-25 age group, 89% would rather use a debit card as would 87% in the 25-40 group, *Digital Transactions News* reported in July. That dips to 54% for those 57 or older. Regardless of age group, 78% would choose a debit card instead of a credit card.

"Consumers are looking for payment methods for the way they're interacting with things online today," Rezaiezadeh says. "Account-to-account has been built specifically to enable payments online. It's less about the underlying rails, more about the service enabled."

That echoes Nelsen's thinking about the importance of real-time payments. "Over time, we're very optimistic there will absolutely be benefits in going from batch to real time," he says.

DEALING WITH DISPUTES

And that speaks to the state of account-to-account transactions riding on real-time payment rails. It's early days for the United States. The two prominent real-time payments networks—Early Warning Services LLC's Zelle focuses on peer-to-peer payments and The Clearing House Payments Co. LLC's Real Time Payments Network is commonly used for bank-based transactions—only launched in 2017. A third major one, the Federal Reserve's FedNow, is expected to launch in 2023.

Much needs to be worked out before account-to-account transactions could be a wholesale replacement for some card transactions. One issue is fraud and chargebacks. Today, issuers lean toward aiding the cardholder in these situations and the process is mostly the same across cards, despite differences among issuers.

Account-to-account transactions have no shared fraud or chargeback process. "There really isn't one well-defined scheme at scale to support some of these more complex e-commerce flows," Nelsen says. Not much is needed for very simple use cases, but e-commerce can be complex, involving subscriptions, delayed delivery, multiple recipients, and shipping addresses.

Real-time payments work well for P2P payments or sending money from one bank account to another, Nelsen says. With e-commerce purchases involving non-digital goods, however, funds can be sent, but the consumer may have an issue with the product or service. "If something doesn't work, you have to have a way to reconcile that," Nelsen says. "You need some way to handle the cardholder dispute."

Consumers may know some merchants they trust to make them whole, but other sellers may not be as likely to accommodate refunds or make-goods. That could mean consumers are less likely to provide direct account access to merchants outside of that trusted circle.

Despite issues like these, GoCardless is not shy about its ambition to build a global network for account-to-account transactions, Rezaiezadeh says. The card networks already have global networks. "The question for me is whether [the card networks] can make these things work together," he says. "The second part is can they do that while maintaining their market share and profitability for the card products." DT

> "A lot of merchants today have moved to a recurring-revenue business model, like subscription or card-on-file."
> —**SIAMAC REZAIEZADEH**, DIRECTOR OF PRODUCT MARKETING, GOCARDLESS LTD.

WHY THE E-COMMERCE METEOR WILL BURN BRIGHT POST-PANDEMIC

Consumers have turned to mobile and desktop buying in record numbers. Merchants and processors are figuring out how to sustain the surge.

BY **PETER LUCAS**

E-COMMERCE HAS BEEN booming since the start of the Covid-19 pandemic and is showing no signs of slowing down. In 2021, online consumer spending totaled a record $855 billion, up 9% from 2020, according to Adobe Inc.

Myriad factors are driving the surge in online spending. One factor is that consumers are buying more everyday products online, such as household items and groceries, which in turn has increased the frequency of their online purchases.

Another factor is a growing preference for buy online, pick up instore options (BOPIS), as they afford consumers the convenience of not only buying online but also knowing the item will be waiting for them in-store the same day, rather than expecting to have it delivered.

And yet another trend embedding online purchasing in consumers' daily lives is online meal ordering. For many restaurants, online ordering for take-out or delivery has become a must as consumers' willingness to dine out has ebbed and flowed with the unpredictable nature of the pandemic.

With these new online-shopping habits firmly ingrained, payments experts predict consumers will not revert to their pre-pandemic patterns one the pandemic subsides.

A 'DAILY ACTIVITY'

"A year ago, questions were raised about whether consumers' online buying habits would stick post-pandemic. A year later, the stickiness of e-commerce is not going down," says Chris Abele, vice president for Carat and digital commerce strategy at Fiserv Inc. "The convenience and speed of e-commerce continues to win over consumers and create compelling user experiences that keep consumers coming back."

Online sales for the 2021 holiday shopping season show just how ingrained e-commerce has become in consumers' lives. From Nov. 1 through Dec. 31, consumers spent $204.5 billion, up 8.6% from the same period in 2020, according to the Adobe Digital Economy Index. During that period, e-commerce sales surpassed $3 billion in daily spend a record 38 days, compared to 25 days in 2020.

Helping drive that trend was that consumers spread out their online purchases during the holiday-shopping season. This contrasts with the former pattern of spending primarily on the traditional big holiday sale days, such as Black Friday and Cyber Monday.

Plus, consumers began their holiday shopping earlier. Online sales during the three and a half weeks before Thanksgiving increased more than 19% compared to the same period in 2020, while sales the five days between Thanksgiving and Cyber Monday, also known as Cyber Week, were down 1.4% from a year earlier, according to Adobe.

Of particular note about 2021 online holiday sales is that they grew despite persistent bottlenecks in the supply chain that have sparked inflationary prices and increased the appearance of out-of-stock messages on merchant Web sites for certain items.

Consumers saw more than 6 billion out-of-stock messages online this past holiday shopping season, a 10% increase from 2020 and more than twofold compared to 2019, according to Adobe.

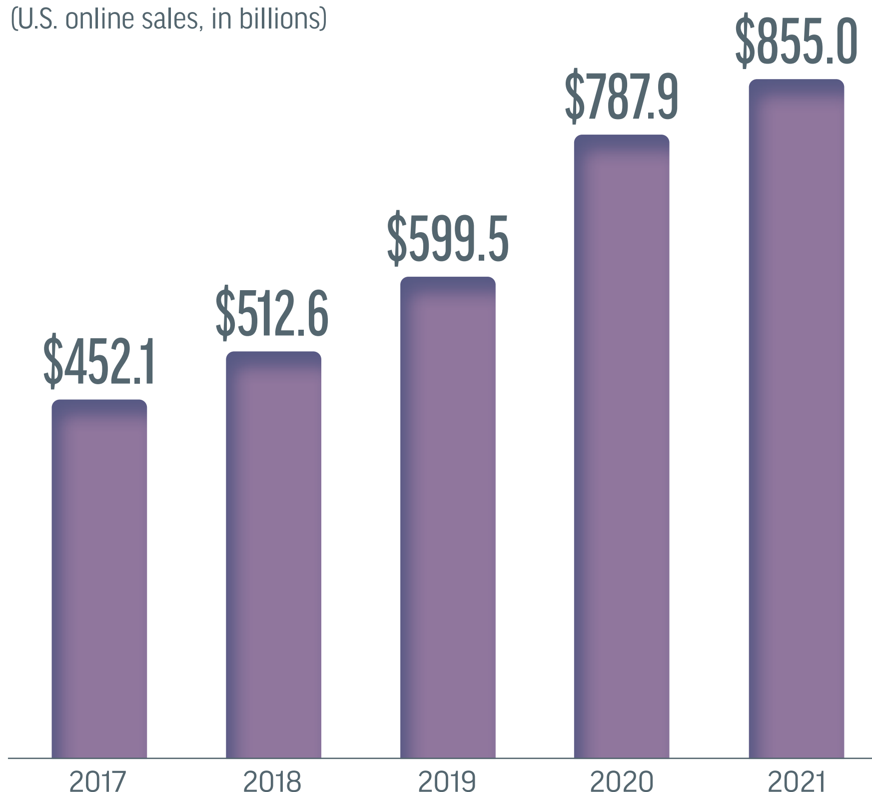
"This holiday-shopping season was the first time where big promotional moments like Cyber Monday and Black Friday took on less of the spotlight," says Taylor Schreiner, senior director, Adobe Digital Insights. "E-commerce has become a ubiquitous daily activity and a flexible way for shoppers to navigate product availability and higher prices."

With surges in the pandemic being driven by new variants of the Covid-19 virus, changes in online buying habits continue to be reinforced, which in turn lessens the odds consumers will revert to their pre-pandemic online-purchasing habits once the pandemic ends.

"The pendulum on consumer online buying habits may swing back a little once the pandemic subsides, but not by much," says Ginger Schmeltzer, a strategic advisor for Aite-Novarica Group, a Boston-based consultancy. "At the outbreak of the pandemic, a lot of consumers, especially those that were most vulnerable, turned to online shopping out of necessity, but since then, they have found it beneficial enough to continue embracing it."

Another trend to emerge during the pandemic is that processors are seeing different buyer profiles. For example, ACI Worldwide Inc. is seeing greater spreads in the time of day online shoppers are interacting with e-commerce sites, the products they purchase, and the type of sites with which online shoppers interact.

"Online gaming has been very popular during the pandemic, and we are seeing more daytime visits to gaming sites," says Amanda Mickleburgh, director for product merchant fraud at ACI. "We've also seen changes in the types of devices



being used to make online purchases, including devices connected to the Internet of Things."

A BOPIS BOOST

With the gains made during the pandemic expected to stick, payment experts say merchants need to do more to meld the online and in-store sales channels if they want to continue to benefit from those gains, as consumers have shown they will move freely between the two.

"E-commerce is critical to a merchant's business, especially small and medium-size businesses, because without it they will miss out on a segment of consumers that prefer to shop entirely online or start in one channel and end in the other," says Afshin Yazdian, chief executive, U.S. acquiring, for Paysafe Ltd. "It's also a way for smaller merchants to compete with big retailers. If a merchant lacks an e-commerce channel, it can hurt their business."

One way merchants can effectively meld the online and in-store channels is by enabling BOPIS. Aite's Schmeltzer cites the example of a local bookstore that adopted a BOPIS model early during the pandemic, when many consumers were avoiding stores that did not sell essential items such as food and bath products.

"It's an example of how far downstream BOPIS is moving and how creative storefront merchants are becoming with e-commerce since Covid," Schmeltzer says.

Another indication of how ingrained BOPIS has become is how larger retailers have expanded the space dedicated to it. "BOPIS has become a permanent feature for big-box merchants. It's table stakes now," says Claude Clausing, chief business development officer for Exact Payments, a Scottsdale, Ariz.-based processor specializing in e-commerce.

The recent holiday-shopping season shows just how important BOPIS has become to merchants. Retailers that offer in-store/curbside pickup saw that fulfillment option used for 23% of all online orders during the holiday shopping season, down slightly from 24% in 2020 but up from 22% in 2019, an indication that demand for the service remains steady, according to Adobe.

On Dec. 23, the percentage claimed by in-store/curbside pick-up orders placed surged to 40%. In addition, curbside orders averaged $91, with 2 items typically in the shopping cart, Adobe says.

MULTICHANNEL SHOPPING

Further enhancing the appeal of e-commerce is that consumers can initiate a search for an item online at various merchants in a 20-mile radius of their home, for example, to see which has the item in stock and price compare. The shopper can order and pay online, then pick the item up same day.

"This way, a consumer doesn't have to go to multiple stores searching for an item," Schmeltzer adds. "Instead, consumers can start in one channel and finish in another. Merchants are getting comfortable with the idea that there is more than one channel for servicing customers."

Another sign that the gains e-commerce has made during the pandemic will stick is that most small merchants that did not have an online presence prior to the pandemic have established one. In addition, those with previously modest online stores are beefing them up.

Many small merchants lacking the resources to launch their own e-commerce store are turning to online marketplaces, such as Amazon.com, to launch a store and help with delivery logistics, Mickleburgh says.

"We've also seen merchants expand or set up stores on social-media sites and use social media to promote those stores," she adds.

The buy now, pay later (BNPL) trend ("The BNPL Phenomenon," October 2021) is also helping to fuel the popularity of e-commerce. During the past two years, slews of merchants have added BNPL as an online payment option, as well as in-store.

Revenue form BNPL orders rose 27% during the 2021 holiday shopping season compared to 2020, according to Adobe. At the same time, the number of online purchases paid for using BNPL during this period rose 10%, compared to 2020. On average, consumers using BNPL spend $224 and place about three items in their shopping cart, Adobe says.

"Adding more alternative payment options like BNPL and mobile wallets is a way for merchants to add value online," says Fiserv's Abele.

To illustrate his point, Abele says that many online grocers serviced by Fiserv have added acceptance of electronic benefits cards to their sites.

"EBT cards can account for 15% to 20% of a grocer's in-store sales, but you didn't see them accepted online by grocers pre-pandemic," he says. "Now, nearly all grocers with an online presence accept them. Without that acceptance, they would not be able to connect online with the demographic that uses EBT cards."

A B2B BOOM

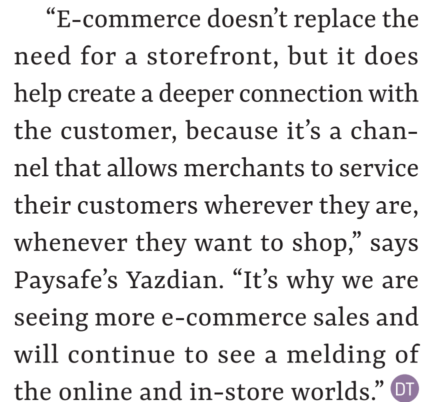
One area of e-commerce that tends to get overlooked is business-to-business sales. Traditionally, B2B suppliers have been slow to embrace e-commerce, especially if they have an electronic data interchange network to which buyers can connect. While barriers to B2B e-commerce were falling prior to the pandemic, that trend has picked up the past couple of years.

"We have seen a boom for B2B e-commerce," says Nic Beique, founder and chief executive for Helcim, a Calgary-based processor. "A lot of check-based transactions are moving to e-commerce. We are also seeing more online invoicing."

Beique adds the majority of Helcim's transaction volume consists of card-not-present transactions. The current breakdown is 60% CNP and 40% card present, whereas pre-pandemic it was evenly split.

While Helcim has rolled out several e-commerce tools for B2B suppliers during the pandemic, Beique adds that, surprisingly, B2B buyers are frequently using mobile devices to make purchases, an indication of how deeply e-commerce is taking root in this space. "We thought [our B2B e-commerce volume] would be more desktop-driven," Beique adds.

Just as processors are adding more alternative payment options for e-commerce merchants, the same trend is occurring in B2B. Exact Payments, for example, plans to offer its B2B suppliers non-card-based payment options, such as ACH and real-time payments.



With all indications pointing to online purchasing being deeply ingrained in consumers' consciousness, many observers say merchants and B2B suppliers that don't offer an e-commerce store are at risk of losing their connection to customers, even those who still frequent the storefront, payment experts say.

"E-commerce doesn't replace the need for a storefront, but it does help create a deeper connection with the customer, because it's a channel that allows merchants to service their customers wherever they are, whenever they want to shop," says Paysafe's Yazdian. "It's why we are seeing more e-commerce sales and will continue to see a melding of the online and in-store worlds." DT

ePProcessingNetwork.com
The Everywhere Processing Network®
800-296-4810

Contactless/NFC
PIN Debit
Inventory
Cash Discount
LEVEL II & III
Multi-Merchant
QuickBooks® Sync

SHOULD CBDCs BE THE NEXT BIG THING?

Governments are moving closer to issuing digital money. That could introduce some benefits—but also many risks and complications.

BY ERIC GROVER

CENTRAL BANK DIGITAL CURRENCIES (CBDCs) ARE COMING, slowly but inevitably. They can be retail (for use by consumers and businesses), wholesale (for use between financial institutions), or both. Evangelists enthuse they'll improve money and domestic and cross-border payments. At this juncture, however, such compelling use cases are unclear.

Federal Reserve notes (cash) and reserves at the Fed are central-bank money, in other words, Fed liabilities. Banks already transact in central-bank money among themselves. The public primarily uses commercial-bank money.

Retail CBDCs enable consumers and businesses to hold, and transact in, electronic payment instruments—but in national unit accounts that are central-bank rather than commercial-bank labilities.

Launched in 2014, the first CBDC, Ecuador's central bank's digital dollar, was shuttered in 2018. The dinero electrónico failed because of its reliance on the state mobile network operator for distribution and because of distrust of the central bank.

Notwithstanding the dinero electrónico's demise, central banks are increasingly keen on CBDCs. Their interest in the matter has been accelerated by such factors as the rise of cryptocurrencies, Facebook's 2019 announcement of the stablecoin Libra (rebranded Diem), and the People's Bank of China's commitment to developing an e-yuan.

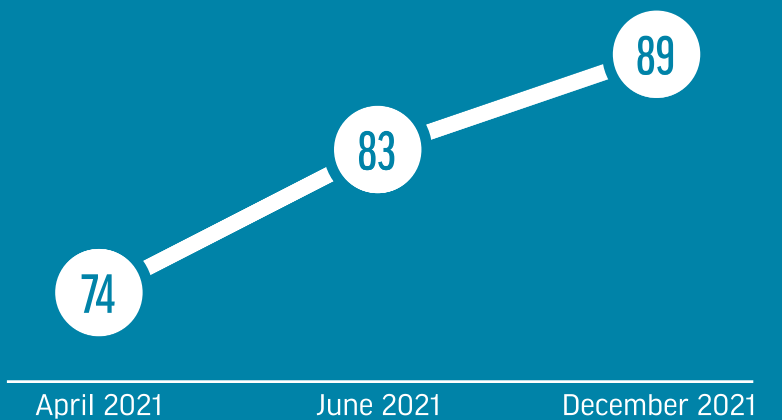
Debuting in October 2020, the Bahamas' digital sand dollar was the second CBDC out of the gate. The Caribbean Central Bank's digital dollar has been introduced in seven out of eight served island countries and territories. And Nigeria's central bank has started issuing e-Naira.

WHAT ABOUT THE FED?

Most of the world's major central banks will follow suit. The highest-profile CBDC pilot these days is the PBOC's e-yuan. It reports

FAST RISE

(Number of countries in various stages of CBDC development, from research to launch)



Source: Atlantic Council

more than 140 million digital-wallets for managing e-yuan have been downloaded, 10 million acceptance-ready merchants, and 150 million transactions to date, totaling almost $10 billion.

To be sure, China's central bank says it wants to improve payments efficiency beyond what Alipay, China Union Pay, and WeChat Pay have achieved. But an e-yuan could provide additional benefits for Beijing. In a Financial Times interview, the UK's spy chief, Sir Jeremy Fleming, warned that the digital renminbi could be a tool to surveil users and exert control over global currency transactions.

The Fed has been studying the development of an electronic greenback. But the Fed is a creature of Congress. Fed chairman Jay Powell declared, "We would not proceed" adopting a digital dollar "without support from Congress ... ideally ... in the form of an authorizing law."

Almost 10,000 banks and credit unions compete to serve Americans.

Washington can ban private digital currencies or use regulation to tilt the playing field, either of which would suppress money-and-payments innovation.

Milton Friedman's counsel a quarter century ago that the future of e-cash would depend on the private sector's "flexibility to experiment, without broad interference by government" should inform Congressional policymakers. Ideally, CBDC legislation would provide legal and regulatory clarity, be technology-agnostic, and prohibit regulators from handicapping private digital currencies.

But the Fed isn't of one mind. Powell remains undecided. Vice chair nominee Lael Brainard is a CBDC proponent. Governor Christopher Waller and former vice chair of supervision Randal Quarles are skeptical there's a compelling need, noting the U.S payment system is already substantially digital and works well.

Waller and Quarles also argue that the pro forma arguments trotted out in a Fed e-dollar's favor—that it's necessary to promote financial inclusion and to defend King Dollar against a digital yuan—don't bear scrutiny.

The percentage of unbanked American households has been falling, going from 8.2% in 2011 to 5.4% in 2019. Significantly, 75% of these households say they don't want a bank account. Almost 10,000 banks and credit unions compete to serve Americans. Neobanks like Chime and Green Dot, and de facto banking from Square and PayPal, continue to make it ever easier to bank.

DESIGN CHOICES

But if Washington wants to do more than recite financial-inclusion pieties, it would lower barriers to entry in financial services and repeal debit-interchange price controls.

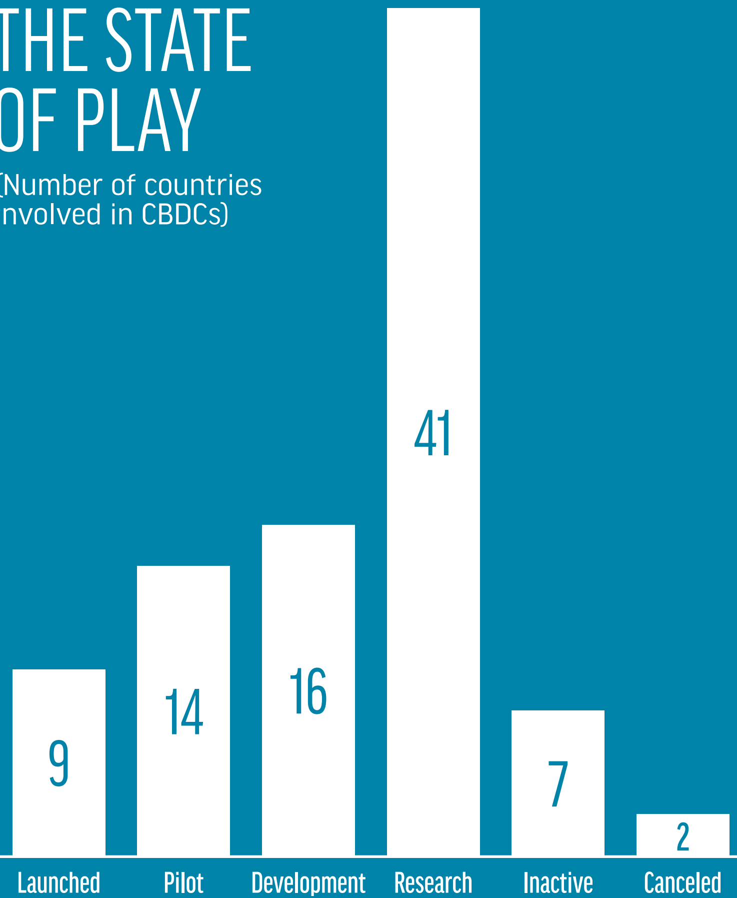
THE ONLY MAGAZINE COVERING THE TOTAL PAYMENTS MARKET

In 2019, there were 150.2 billion digital transactions in North America. *Digital Transactions* magazine covered them all. It is the only publication addressing the total market.

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

Covering the electronic payments business for 18 years, *Digital Transactions* magazine is your independent source for changes affecting the payments market. *Digital Transactions* is also available in a digital edition on our web site, DigitalTransactions.net

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



Source: Atlantic Council

These moves would more effectively expand financial-services access than a Fed e-dollar.

Design choices will affect CBDCs' utility and impact. CBDCs can be account- or token-based. Account-based systems would be easier to implement, whereas token-based systems should enjoy greater flexibility.

The banking and money system is a two-tier one. The Fed serves banks, and banks serve consumers and businesses. Champions of the idea that government should take a greater role in banking advocate the Fed should provide bank services to consumers and businesses directly, competing with commercial banks. Alternatively, as with physical cash, the Fed could rely on banks to distribute e-dollars.

CBDCs can be supported by permissioned-distributed, hybrid, or central electronic ledgers. Central banks will weigh tradeoffs differently and employ different architectures. No CBDC will be unpermissioned.

While the digital sand dollar is limited to domestic use, electronic dollars, euros, and pounds, probably won't be. Most greenbacks circulate outside the United States. While an e-dollar won't be anonymous, its value would likely be greater abroad.

A Fed e-dollar's domestic impact likely would be modest. However, CBDCs could roil the cross-border payments market, making transfers faster, more convenient, and cheaper, thereby boosting demand.

A digital King Dollar may supplant weak national currencies and payment systems. If Venezuelans and Zimbabweans, using smart phones, can transact in e-dollars rather than bolivars and Zimbabwean dollars, respectively, many will, and will be better off for it.

RISKY BUSINESS

Cheerleaders say central-bank money is less risky, but in countries like Venezuela and Zimbabwe, central-bank money is plenty risky. And, in the U.S., private digital currencies—backed one-to-one by dollars in FDIC-insured accounts and short-term, liquid securities—wouldn't be materially riskier than Fed e-dollars.

Libertarians love payments anonymity. No CBDC, however, will be anonymous in the way cash is. For governments, that's a plus. For consumers and businesses, not so much. Digital dollars and pounds, however, are likely to offer greater privacy protections than digital yuan.

CBDCs pose risks. They'll be easier for consumers and businesses to hold and transact in than cash, and, therefore, will reduce banks' assets and lending capacity. In a normal interest-rate environment, that wouldn't be a big risk. Additionally, in uncertain times, there's risk of capital flight from banks to CBDCs.

It's too early to know how they'll affect central banks' ability to implement monetary policy. Advocates contend policy tools could be enhanced. With the elimination of physical cash, CBDCs would enable negative interest rates. Congress should take care to prevent the possibility of negative rates being

A QUICK PRIMER ON CENTRAL BANK DIGITAL CURRENCIES

CENTRAL BANK DIGITAL CURRENCIES ARE DIGITAL TOKENS representing a national fiat currency. They are issued, as the name implies, by the nation's central bank, which must maintain reserves against them. About 90 nations have at least looked into the technology, while nine have launched a CBDC, according to the Atlantic Council (chart, page 24).

While CBDCs are stablecoins by definition (tethered to the value of a national currency), they differ from privately issued stablecoins ("The Price of Stability," December) in that they may nor may not be created through a distributed ledger like a blockchain. Some experts, however, argue there's little to be gained in managing a national digital currency through the public/private key pairs generated via a blockchain. "It's unlikely a central bank would manage a currency in such a fashion," says Tim Sloane, vice president, payments innovation, at Marlborough, Mass.-based Mercator Advisory Group.

While many countries have contemplated digital currencies for some time, observers say Facebook Inc.'s announcement of its Libra project in the summer of 2019 may have catalyzed research and development in a range of national governments. The project, which proposed a digital currency backed by bank deposits and short-term government securities, attracted immediate and withering criticism from banking regulators around the world, driving out many of the project's original 27 corporate backers and forcing Facebook (now Meta) to rename and redesign the project.

The currency, now known as Diem, may have assumed far more modest goals, but some observers say it has left a legacy among the world's central banks, many of which have stepped up their investigation of CBDCs. Just last year, the number of countries in various stages of implementing or investigating the technology grew from 74 in April to 89 in December, according to the Atlantic Council. "Facebook launching Libra started it all," says Talie Baker, strategic advisor at Aite-Novarica Group, Boston.

The advantages of a CBDC include the ability to speed and, arguably, simplify transactions that formerly would have required checks, paper money, or coins. The currency's digital properties would presumably simplify the central bank's management of money and give consumers a currency they could keep in an app, just like cards. "Here's a currency everyone can use that's cheaper," says Aaron McPherson, a long-time payments analyst and principal at Aaron McPherson consulting. "I'm an advocate of stablecoins in general and CBDCs [in particular]."

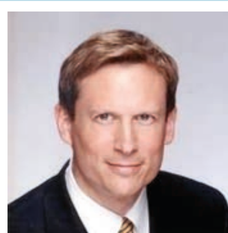
But critics aren't so sure a CBDC, in the United States at least, portends well. The concept would inject the Fed into retail transactions for the first time, since the central bank would issue the tokens and carry them on the books as liabilities. That role is one the Fed is ill-suited for, critics argue.

Meanwhile, a Fed currency based on blockchain would be a step back, say some observers. "We looked at blockchain technology when we built" the Real Time Payments network, says Rob Hunter, deputy general counsel at The Clearing House Payments Co. LLC. "If it worked well for payments, we would have used it, but it doesn't."

And there are "some real daunting problems" associated with a government-issued digital currency, even without a blockchain, Hunter argues. These include data collection by the government and its potential for invasions of privacy and concerns about information security and terrorist financing. "Right now, it would be hard to bring the entire banking system down in one fell swoop," he says. But with a CBDC, "it becomes much more susceptible to attack," Hunter adds. "It's the consummate honey pot for terrorists."

Meanwhile, critics argue, there's nothing wrong with the nation's payments systems that a CBDC could fix. "There are a lot of different ways to move money in the United States, and we are all blessed with that," Hunter says.

—John Stewart



'Right now, it would be hard to bring the entire banking system down in one fell swoop. [But with a CBDC] it becomes much more susceptible to attack.'

—ROB HUNTER, DEPUTY GENERAL COUNSEL, THE CLEARING HOUSE PAYMENTS CO. LLC

Historically, innovation in money and payments has been driven by private initiative, not by the state.

designed into a Fed e-dollar. Enabling negative interest rates, thus punishing savers and causing malinvestment, is a bug, not a benefit.

CBDCs may have different velocities than cash. And competing private payment systems self-correct. Public systems are quite another matter.

Indeed, the biggest CBDC risk is that they could pre-empt or crowd out the development of competing private digital currencies. The Fed is the financial system's paramount regulator and enjoys virtually unlimited resources. Commercial banks, fintechs, and payment networks will, consequently, be reluctant to compete against it.

Fed Governor Waller observes that "markets operate efficiently when private-sector firms compete to provide the highest-quality products to consumers and businesses at the lowest possible cost" and that "government should compete with the private sector only to address market failures." There's no obvious failure in payments and bank money.

Quarles, the former vice chair of supervision, warned "a Fed CBDC, or even plans for one, might deter private-sector innovation by effectively "occupying the field."

A LEVEL FIELD

Historically innovation in money and payments has been driven by private initiative, not by the state. In the 7th century, Chinese merchants introduced the first paper currency. It was Scottish banks that invented overdrafts, and multicolored and double-sided banknotes.

Financier Frank McNamara launched the first general-purpose payment card network, Diners Club. Banker Dee Hock was the father of the global bank card network, Visa. Banks built the global cross-border payment-messaging network Swift.

Peter Thiel and Max Levchin founded PayPal. Cryptocurrency pioneers Chris Larsen, Jed McCaleb, Vitalik Buterin, and Anatoly Yakovenko, didn't work at the Treasury Department. Stablecoin development, too, has been spearheaded by private-sector capital and initiative from entrepreneurs like Circle's Jeremy Allaire, Paxos's Charles Cascarilla, Andrew Chang, and Richmond Two, and Tether co-founders and Mastercard Foundation alumni Brock Pierce and Craig Sellars, and entrepreneur Reeve Collins.

Leading CBDCs and stablecoins won't be national silos. Eventually, they'll interoperate, enabling instant cross-border value exchange through global clearinghouses, bilateral or multilateral connections, or both.

In "Denationalisation of Money: The Argument Refined: An Analysis of the Theory and Practice of Concurrent Currencies," Freidrich Hayek advocated free trade in money for private and national currencies to be able to freely compete, subject to market discipline. Fed e-dollars, Citi e-dollars, Diem, ECB digital euros, Circle's USDC, Tether's USDT, et. al., vying for pride of place in e-wallets and different use cases, would foster innovation, with the market guiding development and picking winners and losers.

Best case, competing private and public money and payment systems operating on a level legal and regulatory playing field, will evolve, delivering ever-greater value. DT

Eric Grover is principal at Intrepid Ventures, Minden, Nev.

Co-Branded E-Mail Marketing

Get the Results You Need

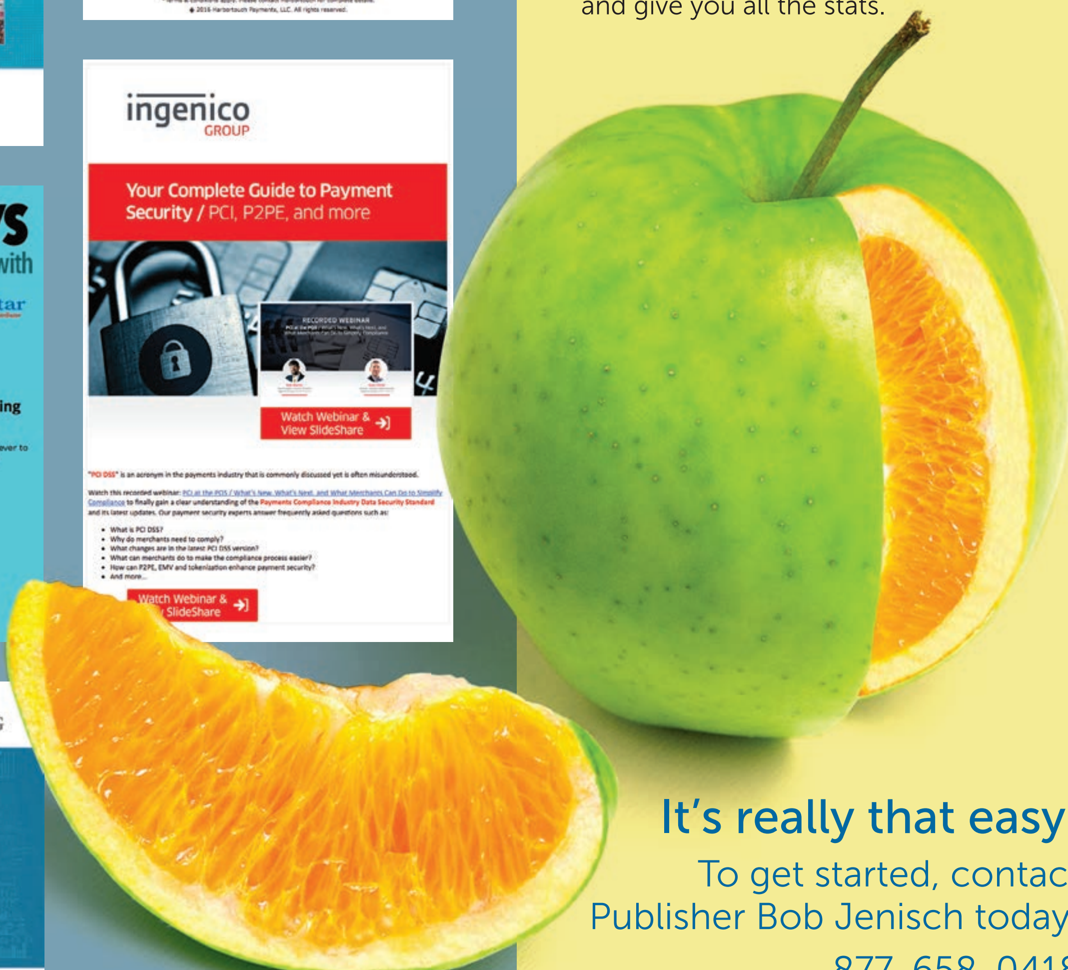
Here's how it works:

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

You give us your HTML creative.

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

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



It's really that easy!

To get started, contact Publisher Bob Jenisch today:

877-658-0418
bob@digitaltransactions.net

security

TOP TIPS FOR PREVENTING ACH CREDIT FRAUD

It's become more common and harder to detect. Here are some measures that can help cut it down to size.

BY **JEREMIAH BENNETT**

Jeremiah Bennet is director of information security at Corpay.

FORCED TO WORK FROM HOME during Covid-19, accounts-payable departments have accelerated plans to move away from paper checks and pay more of their suppliers through the automated clearing house. That, in turn, accelerated another trend: fraud. Through social engineering, fraud attacks on ACH credits are most commonly known as Business Email Compromises, or BECs.

According to the 2020 AFP Payments and Fraud Control Survey Report, for the first time, in 2019, BEC schemes were the most common type of fraud attack experienced, with 75% of organizations experiencing an attack and 54% of those reporting financial losses. ACH credits—outgoing payments from buyer to supplier—were targeted in 37% of BEC schemes.

The problem only got worse in 2020. In the September edition of their Fraud in the Wake of COVID-19 Benchmarking Report, the ACFE reports that 90% of respondents have seen an increase in cyber fraud frequency from July through August. This included BECs.

Three-quarters of respondents said that preventing and detecting fraud has become more difficult in the current environment, and more than 90% expect attacks to increase. Organizations are under siege, and nearly one-third have received no guidance from banking partners about mitigating ACH credit risks.

REDUCING RISK

What can organizations do?

Defeating BECs requires a multipronged approach. Ongoing antifraud training is important because these emails are getting more convincing every day. Fraudsters have become experts in user data and A/B testing, which reduces elements that alert their victims to illegitimate changes to their accounts. Strong internal controls are also important along with network security, which

prevents parties from gaining access to internal systems.

Here are four ways to reduce your ACH credit fraud risk:

1. Handle with Care

Thwarting ACH credit fraud is all about handling supplier banking data securely, which accounts payable must have on hand to transmit their payment file to the bank. This data is often stored in the enterprise resource planning (ERP) system, or sometimes on an Excel spreadsheet, where AP staff has been recorded during supplier onboarding. Sometimes it's stored when a supplier updates its information. Fraudulent change requests are one of the most frequent avenues of attack.

Let's say you've got a new person in accounts payable who isn't fully trained yet. This person gets an email from a supplier, asking to update their bank-account information. Your new hire, eager to please, fulfills the request, inputting a new routing number and bank account, unaware that a million-dollar payment to that supplier is going out the next day. Nobody realizes what's happened until two weeks later, when the real supplier calls asking for payment.

Bennett

> "There really is no perfect system in place, which is why we're seeing ACH credit fraud rise in tandem with the rise in ACH payments."

By then, it's too late to reel ACH payments back in. You can call the FBI and the bank. They may try to help you, but if the thieves are sophisticated enough, they've already moved the money to offshore accounts, and it's completely gone.

2. Secure Information

You should never use an unsecured email for banking information updates, although a surprising number of companies still do. It's too easy for a hacker to intercept one of those emails and use the information in it. If they get contact or bank-account information, they can pose as legitimate suppliers and circumvent internal controls. Some businesses even keep information in spreadsheets or their ERP systems, but systems like these aren't designed to store data securely.

The payments market is large and fragmented.

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

Concise, clean interface is easy to navigate

Breaking news from the payments market, posted daily

Calendar of industry events

Complete current and past issues of *Digital Transactions* magazine

Detailed listings of payments market suppliers

13 years of payments news and analysis

DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

Some companies allow suppliers to update their own information in supplier portals. That might work, provided that companies manage secure portal access and verify all updates. However, if suppliers can log in and update information, it's likely that hackers can access the same information with very little resistance.

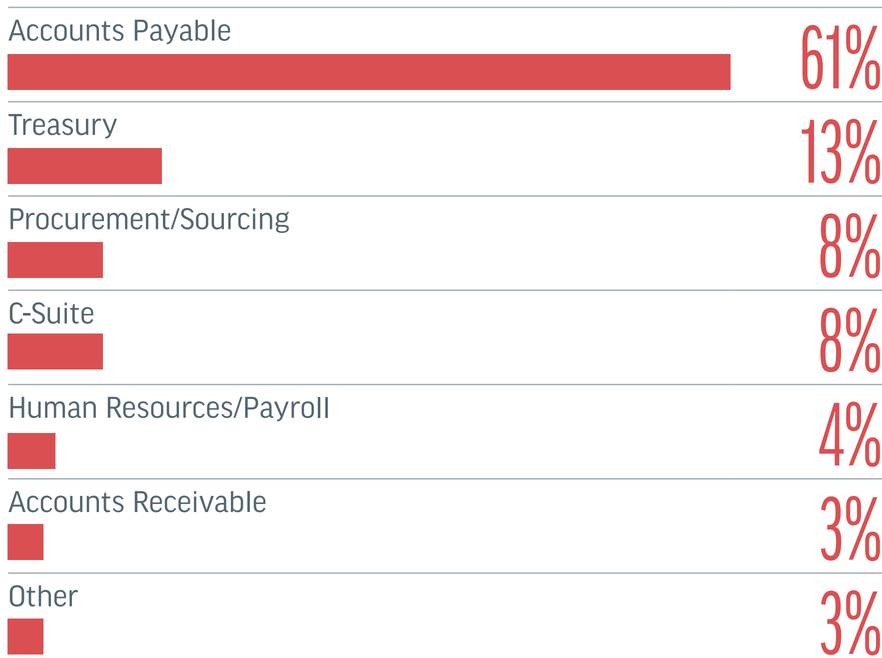
The most sophisticated approach I've seen so far includes a trained procurement team that verifies and validates all changes that come through. But there are a couple of drawbacks to this approach. It's a big IT investment with plenty of labor asks. Even then, it's still prone to internal fraud. At the end of the day, even the best systems will still have their risks. The goal is to minimize them.

3. Look at Fees

Companies often try to shift the risk and time burden to others, with some success. For example, they may choose to pay their suppliers by card, which puts the risk on credit card networks. In cases of card fraud, it's more likely that payments can be canceled or refunded.

Virtual cards offer even more security because they provide unique numbers, which can only be used by a specified supplier for a specified amount. The big drawback is that not all suppliers accept cards—there are fees to consider.

An organization I'm familiar with pays many of its suppliers with PayPal. Its suppliers—most of them small businesses—are located around the world. AP doesn't have the time or staff to verify payment information, validate bank accounts, and deal with ongoing updates. As the intermediary, PayPal handles all that and guarantees that the funds go to the right place.



VULNERABLE ENTITIES

(Corporate departments reporting business email compromise attacks)

Department	Share
Accounts Payable	61%
Treasury	13%
Procurement/Sourcing	8%
C-Suite	8%
Human Resources/Payroll	4%
Accounts Receivable	3%
Other	3%

Source: Association of Financial Professionals 2021 Payments Fraud and Control Report

But, here again, suppliers pay a hefty fee—in the neighborhood of 3%.

4. Shift the Risk

There really is no perfect system in place, which is why we're seeing ACH credit fraud rise in tandem with the rise in ACH payments. But there is a perfect way to shift the risk to companies that are built to withstand the verification and validation burdens.

SOPHISTICATED ATTACKS

Today's payment-automation providers manage supplier information, so individual companies no longer have to spend valuable time on it. It's similar to handing the reins to IT and procurement departments to lock down the database and institute controls. The difference is that working with a provider removes the time investment and liability.

Think of payment-automation providers as a means to outsource risk. Their sole focus is to ensure secure, on-time payments to your suppliers without causing costly overhead. They have perfected the systems and processes for hundreds of thousands of AP departments across the United States, and in ways that businesses would be hard-pressed to replicate.

Businesses used to worry about check fraud above all else. While they still have to pay attention to that threat, it's become a low-tech form of fraud that's easy to understand and plan for. As companies shift to electronic payment methods, they're increasingly experiencing sophisticated cyberattacks, which target much larger sums and are harder to defend against. With such attacks growing, businesses may find that outsourcing to professionals is the best defense. DT

WHEN FRAUDSTERS TAKE A VACATION

Theft of loyalty points has become a serious issue in the travel industry. But is it being taken seriously by hotels and airlines?

BY **YOHANNA ANDOM**

Yohana Andom is senior product manager at Forter Inc., New York, N.Y.

WITH A NEW YEAR comes new optimism that there will be a return to activities like travel. Some consumers will log in to book travel for the first time in a while, or to revisit rewards points, and it'd be a terrible surprise to find out they have been compromised by online fraud.

The word "fraud" has many associations. such as the image of a hacker tapping into someone's social-media profiles or thieves who ring up large bills on a consumer's credit card. For retailers, issues with policy abuse, such as customers "wardrobing" (wearing clothes with the tags on and then returning it despite the item then being ineligible), may be the association.

The goal of a fraudster can vary, from phishing attempts, to racking up a bunch of charges on someone else's credit card to "borrowing" an outfit from a store. However, what about when fraudsters take a vacation?

What about someone intentionally stealing loyalty points?

PERFECT BREEDING GROUND

According to Mordor Intelligence, the global loyalty-management market was valued at $3.2 billion in 2019 and is expected to reach a value of $11.4 billion by 2025. Hotel and airline-industry rewards programs essentially allow their customers to collect points or miles each time a room or flight is booked within the brand.

Travel rewards are like money in the bank. However, unlike actual banks, these are ones consumers trust too much and don't check often enough.

Miles and hotel points encourage many consumers to stick with where they can receive the most "points" as they travel. For those closely making purchasing decisions linked by the rewards—investing their time, money, and energy on brand loyalty —to have the fruits of their labor ripped away would be devastating.

Unfortunately, account takeovers by fraudsters have become quite common within travel industries. In 2020 alone, account takeovers were up 282% compared to the previous year. Combined with lackadaisical password practices and even the most conscientious of customers checking their loyalty-account balances only about once every three months, this is the perfect breeding ground for scammers to cash in on loyalty points.

When travel rewards are stolen, the results can be devastating for customers, as this is the product of

their conscious choice to support a business to achieve the goal of a dream vacation or hotel spot. Organizations that permit this behavior by not taking responsibility for the threat of fraud will also face very real consequences.

While customers have to be more vigilant in protecting their loyalty accounts by checking in more often and practicing good cyber hygiene, travel companies have steps to take as well.

PRACTICAL STEPS

So what can be done about this issue?

1. Leverage the largest possible network to ensure your customer account information is safe. Don't rely only on your internal network; work from a global network.

While no network is fully immune to cybercriminal activity, working from a global network typically means a greater volume of security measures for hackers to infiltrate to get their prize—customers' information and points. The greater size and complexity of the locations in the global network allow organizations to keep data safer than when all is concentrated in one location. In the case of a small and dense network, a cybercriminal needs only to target one site to access customers' accounts.

> Unfortunately, account takeovers by fraudsters have become quite common within travel industries.

2. Automate decisions. Utilize machine learning to instantly distinguish fraudsters and customers.

By incorporating technology intended to catch fraudsters, travel businesses can best monitor for suspicious activity on customer accounts. This also means the business assumes the responsibility to protect their loyal customer relationships, something hotels, airlines, and more should prioritize to ensure long-term business with frequent travelers. After all, the accounts and points will not protect themselves. If a rewards program is promised, the business must be willing to put proper measures in place to protect their offerings. Allocating resources to an automated learning-based platform will save businesses time, energy, and customer relationships in the long term.

3. Streamline the customer experience. Save customers from multifactor authentication by identifying them with precision.

Another part of offering a rewards program is, again, ensuring that the business is able to provide the reward to customers who reach the aspirational number of points. It is not up to the customer to ensure that their points are not swiped out from under them. That's up to the company that offers the grand prize. This is why businesses should aim for a secure strategy to protect their business from fraud that does not require more to do on the customer's end.

If they are signing up for travel arrangements, why should it be on the customer to go the extra mile to have multifactor authentication? Would they still use a business that does if some systems offer simpler, more secure travel programs? Rewards programs should be simple and user-friendly for customers. Don't put it on customers to secure their own accounts when technology is out there to streamline the experience.

The numbers do not lie. The travel industry needs security solutions. Fraudsters have proven they know how to take advantage of vulnerable systems. Companies that protect their customers' loyalty accounts are the ones that are protecting their customer relationships. After all, no lifelong customer wants an explanation of why their dream vacation was compromised. DT

ADVERTISER INDEX

Advertiser	Page	Phone	Website
Digital Transactions	Pages 10, 23, 27, 29	877-658-0418	www.digitaltransactions.net
Electronic Merchant Systems	Back Cover	866-596-8829	www.emsagent.com
eProcessing Network	Page 19	800-296-4810	www.eprocessingnetwork.com
Shift4	Page 1	800-201-0461	www.shift4resellers.com
MagTek	Page 3	562-546-6400	www.magtek.com
Wholesale Payments	Page 5	806-642-4949	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.