

# TRANSACTION

## trends



THE OFFICIAL PUBLICATION OF THE  
ELECTRONIC TRANSACTIONS ASSOCIATION

## Relationships Evolved

From ISVs to APIs, tech-fueled opportunities are reshaping payments partnerships



### ALSO INSIDE:

**A Year of Fighting for Payments**  
PAGE 10

**Payments Facilitators:  
The New Acquiring Method**  
PAGE 12

**Tough Realities of Protecting  
the Cyber Domain**  
PAGE 22

**A Glimmer of Hope for OCP?**  
PAGE 25



**MERCHANTS' CHOICE  
PAYMENT SOLUTIONS**

# BE RELEVANT

## MERCHANT FOUNDRY

*"A Business Solutions Platform"*

*Commercial  
Loans*

*Merchant Security  
& Compliance*

*Social  
Media*

*Cloud  
POS*

*Big Data  
Solutions*

*Loyalty  
Programs*



**Be a part of the most exclusive and sophisticated  
ISO Partner Program in the Industry**



**Call Larry Jones 281-895-5924 [ljones@mcpscorp.com](mailto:ljones@mcpscorp.com)  
Call Jenna Padilla 281-583-4488 [jpadilla@mcpscorp.com](mailto:jpadilla@mcpscorp.com)**

REACH MORE CUSTOMERS.  
EARN MORE REVENUE.  
PARTNER WITH EVO.



**SIMPLIFYING PAYMENTS** AROUND THE  
GLOBE. **130+ CURRENCIES** ACROSS **50**  
**MARKETS** WORLDWIDE.

We support the success of our agents, partners, and developers with global processing solutions, world-class merchant services and integrated payment APIs. EVO resources, combined with competitive pricing and exceptional customer support, enable our partners to cultivate more business opportunities for a healthier bottom line.

PROCESSING OVER **\$100 BILLION** IN CARD TRANSACTION VOLUME ANNUALLY

FACILITATING CARD ACCEPTANCE FOR OVER **400,000 BUSINESSES** GLOBALLY

PROVIDING INTEGRATED PAYMENT SOLUTIONS WITH **EVO SNAP\***



# IMPACT YOUR BUSINESS.

**TRANSACT** is the one show focused solely on the business of payments.

**TRANSACT** is where you will meet the right people, explore new technologies and discover insights and best practices.

**CONNECT** with the payments technology community — the entire sales channel — to move forward in the right direction and grow your business.

## **ATTRACT** the right people.

From ISOs, VARs and ISVs to top acquirers, tech companies, startups and leading financial institutions, TRANSACT attracts the decision makers and innovators and brings them to you.

## **INTERACT** with new technologies.

Explore the most innovative payment technologies from 200+ exhibitors on the TRANSACT show floor, including those in the Payments Next Zone, Mobile Pay Zone and the NEW Payments Innovation Lab.

## **ACT** on insights and best practices.

Formulate your strategy and turn knowledge into opportunity — immediately. At TRANSACT you'll get the best intelligence, not sales pitches. Learn from industry experts on everything from integrated payments and software to sales and security technologies.

REGISTER NOW AND **SAVE 35%** WITH SUPER EARLY BIRD DISCOUNTS!

**TRANSACT**<sup>®</sup>  
POWERED BY ETA

WED MAY 10 • FRI MAY 12  
LAS VEGAS • MANDALAY BAY  
[www.etatransact.com](http://www.etatransact.com)

CONNECTING THE PAYMENTS TECHNOLOGY WORLD

Follow us on social media for Keynote announcements & the latest TRANSACT news.  [facebook.com/etatransact](https://facebook.com/etatransact)  [@etatransact](https://twitter.com/etatransact)  [@eta\\_transact](https://instagram.com/eta_transact)

# contents

The Official Publication of the Electronic Transactions Association Vol. 21 | No. 6

## features

### 12 **Blurred Lines**

*By Ed McKinley*

Although the payments-facilitator phenomenon isn't exactly new, recent research indicates that it is becoming more widespread and is likely to keep growing. As it does, it will redefine businesses in the payments space and add another merchant-acquiring tactic to their strategies.

### 17 **Transaction Trends Exclusive CE Series: 'Open' for Business**

*By Christine Umbrell*

APIs could be the key for banks competing in a mobile-focused economy. But what exactly are they, and how can financial institutions use them to offer greater transparency and convenience to consumers? We explain here—along with cultural and risk-management mindsets that go along with them. (ETA CPPs: After you read the article, take the online quiz to earn two CE credits!)

### 22 **Cyber Security in a Dangerous Time**

With technological innovations moving at wrap speed, why is cyber security still so hard to get right? At the 2016 ETA Strategic Leadership Forum, Gen. Michael Hayden answered that question with a profound and frank talk about the realities of cyber space—and how private-sector businesses can help.

## departments

4 **@ETA** Announcements and ideas from ETA's CEO Jason Oxman

6 **Intelligence** Vital facts and stats from the electronic payments world

10 **Politics & Policy** Timely political, economic, and advocacy updates affecting your business

25 **Comments**  
Could OCP become more evenhanded?

27 **Ad Index**

28 **People** Kurt Strawhecker ponders next steps for payments.

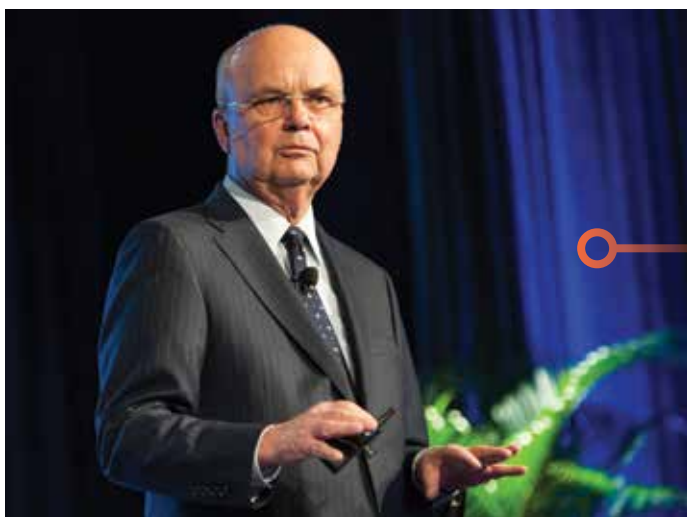


Photo by Great American Photo

## Electronic Transactions Association

1620 L ST NW, Suite 1020  
Washington, DC 20036  
202/828.2635  
www.electran.org

**ETA CEO** Jason Oxman

**COO** Pamela Furneaux

**Director, Education and Professional Development** Rori Ferencic

**Vice President, Strategic Partnerships** Del Baker Robertson

**Director, Communications** Meghan Cieslak

**SVP, Government Relations** Scott Talbott

**Director, Industry Affairs** Amy Zirkle

Publishing office:

**Content Communicators LLC**

PO Box 938  
Purcellville, VA 20134  
703/662.5828

**Subscriptions:** 202/677.7411

### Editor

Josephine Rossi

### Editorial/Production Associate

Christine Umbrell

**Art Director** Janelle Welch

### Contributing Writers

Edward A. Marshall, Ed McKinley,  
Josephine Rossi, Scott Talbott, and  
Christine Umbrell

### Advertising Sales

**Alison Bashian**

**Advertising Sales Manager**

Phone: 703/964.1240 ext. 280

Fax: 703/964.1246

abashian@conferencemanagers.com

### Editorial Policy:



The Electronic Transactions Association, founded in 1990, is a not-for-profit organization representing entities who provide transaction services between merchants and settlement banks and others involved in the electronic transactions industry. Our purpose is to provide leadership in the industry through education, advocacy, and the exchange of information.

The magazine acts as a moderator without approving, disapproving, or guaranteeing the validity or accuracy of any data, claim, or opinion appearing under a byline or obtained or quoted from an acknowledged source. The opinions expressed do not necessarily reflect the official view of the Electronic Transactions Association. Also, appearance of advertisements and new product or service information does not constitute an endorsement of products or services featured by the Association. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided and disseminated with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice and other expert assistance are required, the services of a competent professional should be sought.

*Transaction Trends* (ISSN 1939-1595) is the official publication, published six times annually, of the Electronic Transactions Association, 1101 16th St. N.W., Suite 402, Washington, DC 20036; 800/695-5509 or 202/828-2635; 202/828-2639 fax. **POSTMASTER: Send address changes to the address noted above.**

Copyright © 2016 The Electronic Transactions Association. All Rights Reserved, including World Rights and Electronic Rights. No part of this publication may be reproduced without permission from the publisher, nor may any part of this publication be reproduced, stored in a retrieval system, or copied by mechanical photocopying, recording, or other means, now or hereafter invented, without permission of the publisher.



## A New Year of Payments Innovation

**P**ayments technology is transforming our industry, and your trade association is changing too. Now representing more than 500 companies from across payments, ETA has quadrupled the size of our government affairs and legal teams to address the mounting threats from Washington. Our new sales channel services—including industry guidelines, market research, and business advocacy—are providing merchant sales professionals with more resources and tools than ever. And our ETA Certified Payments Professional (CPP) certification program is newly re-energized—no wonder more than 1,000 of your colleagues have obtained their certification.

ETA's industry activities, policy advocacy, educational content, and events are driving our industry forward. Only ETA has the tools you need to adapt and thrive in the new payments ecosystem. We're excited for future industry partnerships, revolutionary advancements, and disruption of payments as we know it.

In the next decade, we can expect young leaders in payments to shape the landscape of our industry. Millennials are already influencing how we pay, how we shop, and how we ride, which is why ETA has put together a Young Payments Professionals (YPP) Scholar Program, where ETA member company employees between the ages of 21 and 35 can learn more about what makes this industry succeed and get inspired to make it even better. With exclusive invitations to ETA educational sessions and events, introductions to personal industry mentors, and preparation for ETA's CPP exam, our YPP Scholar Program is truly the face of the future of payments.

As the payments landscape evolves, legislators and regulators are taking notice. In October, the Consumer Financial Protection Bureau (CFPB) imposed new regulations on prepaid accounts, limiting access to financial services for the underserved community. The CFPB also swept in new mobile wallets to prepaid regulation, exposing next generation payments services to broad regulatory oversight. Prepaid accounts are one of the fastest growing consumer finance products, and ETA will continue to support and serve our members fighting to help this community.

With fintech innovations coming to market every day, ETA events are the best way to stay on top of our industry's disruption.

It's never too soon to start making your plans to attend ETA TRANSACT, occurring May 10-12, 2017, at Mandalay Bay in Las Vegas. All merchant sales channels—ISOs, PayFacs, ISVs, VARs, and more—will gather in Las Vegas to find the right partners and learn about the products and services that their merchant customers want. Your current and future customers and partners—everyone from the big names to state-of-the-art tech startups—will be at the Mandalay Bay, so seize your space on the show floor, schedule your meeting room, and implement your sales and marketing campaign before the opportunity is gone. With more than 4,000 attendees, TRANSACT is where you come to get serious business done. Contact Del Baker to secure your spot today: dbaker@electran.org.

Now more than ever, ETA membership is vitally important for your business. Only ETA advocates for your business on Capitol Hill. Only ETA has the education and professional certification programs to keep you up-to-date on the latest trends, tools, and opportunities. Only ETA events—and the great discount on attendance that ETA membership provides—give you the networking and connections you need to keep your customers and meet new partners. **TT**







Jason Oxman  
Chief Executive Officer  
Electronic Transactions Association

# Meet the new *iPayment*<sup>®</sup>




## **Better Partner. Better Profits.**

More Agents and ISOs are choosing to partner with iPayment.  
Why? It's simple:

-  One-on-one partner support
-  Superior training and education
-  Maximum earning potential and lifetime residuals
-  Latest payment technologies and value-added services

Contact us today to learn how you can increase your earnings potential.

 866-287-1025

 [newpartner@ipaymentinc.com](mailto:newpartner@ipaymentinc.com)

***iPayment***<sup>®</sup>

## NRF: Post-Election Holiday Spending To Be Second Highest Ever

Consumers plan to spend an average of \$17 less this holiday season compared to 2015, which saw record spending of \$952.58, according to the National Retail Federation's (NRF's) annual consumer spending survey released October 27. And the reason for the more conservative holiday budget this year may have to do with the elections.

"Everywhere you turn—whether you're picking up a newspaper or watching television—political advertisements are taking up ad space that retailers typically use to get holiday shopping on the minds of consumers across the country," NRF President and CEO Matthew Shay said in a press statement. "Once the election has passed, we anticipate consumers will pull themselves out of the election doldrums and into the holiday spirit."

The NRF defines "total spending" as buying gifts for self and others and purchasing food, flowers, decorations, and greeting cards for Christmas, Hanukkah, and Kwanzaa. The survey, conducted by Prosper Insights & Analytics, found that 58 percent of consumers planned to spend average of \$139.61 on themselves, up 4 percent from 2015 and marking the second-



highest level of personal spending in the survey's 13-year history.

Consumers said they will spend \$588.90 on gifts for others and \$207.07 for food, decorations, flowers, and greeting cards this year. They will be shopping both online and in-person, and roughly 57 percent will be visiting these three top shopping "destinations": department stores, discount stores, and online. The survey found 45 percent plan to visit grocery stores/supermarkets; 34 percent will shop at clothing stores; 27 percent will visit electronics stores; and 23 percent will shop at small or

local businesses. Ten percent of shoppers plan to visit outlet stores, a new category added to the survey this year.

What will consumers be shopping for? Sixty-one percent will be buying gift cards, followed by clothing and accessories (54 percent), books, CDs, DVDs, or videos (40 percent—the lowest in survey history as digital downloads replace hard-copy media, according to NFR), consumer electronics (32 percent), jewelry and home décor (both at 23 percent), personal care or beauty items (21 percent), sporting goods (19 percent), and home improvement items (17 percent).

## Infographic

### U.S. Millennials: Instead of using a signature or PIN, which would you prefer to verify your payments?



**67%**

USE FINGERPRINT TO PAY USING CELL PHONE



**67%**

USE FINGERPRINT TO PAY USING PAYMENT CARDS



**58%**

USE EYE SCANS TO PAY



**47%**

USE FACIAL RECOGNITION TO PAY



**46%**

USE VOICE TO PAY

Source: "The Millennials Influence," Vocalink



## Is Cyber Monday Losing Its Luster?

In a report of its November online survey of 1,932 U.K. and U.S. consumers, international payments services provider Computop said consumers are “exhibiting a growing ennui and cynicism when it comes to big day events like Cyber Monday.”

Half of U.S. shoppers and 77 percent of U.K. shoppers are not planning to log in on November 28, according to the study. Why? Both demographics cite lackluster deals. U.S. shoppers said, “The event no longer offers the deals it once did,” while across the pond, shoppers thought deals on the items they would “really like to buy” would not be offered.

## Mobile Optimization Critical to Success During the Holidays

Mobile e-commerce via apps and browsers grew 60 percent from 2014 to reach \$120 billion in 2015, according to Javelin Strategy & Research. Still, the firm reports that “too many merchants” are not optimizing their e-commerce sites or offering flexible payment solutions to improve the customer experience.

In conjunction with the release of its study, “Mobile Online Retail Payments 2016,” Javelin says its research shows that mobile browsers account for far more purchases than native apps such as Uber. In 2015, sales via mobile browsers totaled \$75.3 billion, while native apps sales brought in \$46.9 billion.

“With the holiday shopping season upon us, retailers must stay off of consumers’ naughty list by meeting consumers’ mobile shopping expectations for a streamlined experience and fast and secure checkout options,” advises Emmett Higdon, director of mobile. “Cutting-edge retailers like Adidas, Nordstrom, and Sephora are also using augmented and virtual reality to provide shoppers with mobile-exclusive experiences, enabling them to preview purchases in their own homes and virtually ‘try’ products before making a decision.”

## Consumers Willing To Do More To Prevent Online Fraud

As e-commerce continues to grow, survey results reported by American Express explain how U.S. consumers will take extra steps to protect their personal and payment information.

The “2016 American Express Digital Payments Security Survey” interviewed 1,021 U.S. consumers and 401 merchants. More than half—60 percent—of merchants reported experiencing fraudulent online sales, and 25 percent said incidences of online fraud have increased this year. Participating merchants said an average of 31 percent of online transactions in the past year were abandoned before the sale was completed.

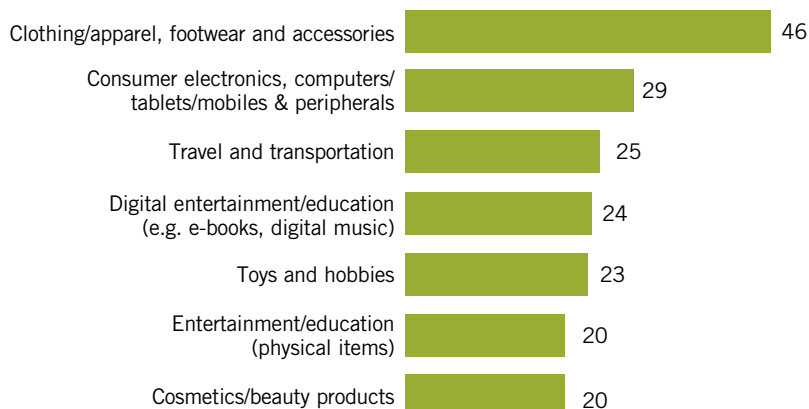
On the consumer side, 48 percent who shopped online in the past year experienced payment fraud. Four in 10 consumers deemed online shopping as riskier than in-store (28 percent). In addition, 42 percent of consumers have abandoned an online purchase due to payment security concerns. The study also showed that abandonment levels skewed higher among younger Gen X and millennial consumers.

Other findings from the survey include:

- Nearly eight-in-10 online consumers (78 percent) are willing to enter their card’s security code; 57 percent of merchants require it.
- While 70 percent of online consumers would answer security questions, 43 percent of merchants have that feature on their websites.
- More than two thirds of online consumers (68 percent) are willing to create a one-time password; 37 percent of merchants require a one-time password.
- For consumers to trust an online merchant, 84 percent want easy-to-find customer service contact information, and 78 percent want visible security cues on a merchant’s website.
- Fifty-two percent of merchants use data encryption on their websites.

## Infographic

### Most Popular Retail Categories for Cross-Border Purchases Globally



Source: “PayPal’s Annual Cross-Border Trade Insights Report 2016”

## Fintech Lending and Financing Revenue To Double by 2020

Global revenue from fintech platforms for lending and financing should double in the next four years to reach \$10.5 billion by 2020, according to Juniper Research. Several factors—including growth in peer-to-peer (P2P) lending; crowdfunding viability; and new analytics platforms—will fuel the increase.

Juniper argued that with credit checking bureaus lacking in emerging markets, social media activity will help lenders assess applicants' riskiness and will factor into overall application decision-making. "Nevertheless, the research cautioned that the process might meet with greater consumer resistance in developed

markets, with many would-be applicants likely to perceive the practice as an unwarranted invasion of privacy," according to the press release.

Juniper also predicted North American and European crowdfunding and P2P platforms will provide more opportunities for individual investment in promising startups, as global interest rates remain at record lows. However, the firm said some analytics platforms may not be sophisticated enough to fully evaluate "distinct corporate operating environments" and their management teams.

"Platform providers need to be transparent about how they assess firms and not just sell the [tempting] potential of funding the next Facebook," research author Michael Lerner said. "We are yet to witness a blockbuster exit for investors, but a successful IPO would cement crowdfunding's foothold in the marketplace."



## Moves & Mergers

**ACI Worldwide** recently appointed Eve Aretakis to executive vice president of application development and Ravi Pochiraju to senior vice president for growth markets. With more than 20 years of senior leadership experience, Aretakis has held executive roles at Siemens and Unisphere Networks. Pochiraju has held senior roles at First Data Corporation, Six Sigma Associates, and Citigroup.

Financial services technology and data platform **Kabbage** announced Amala Duggirala has joined as chief technology officer, and Rama Rao has joined as chief data officer. Previously, Duggirala was executive vice president of global software development and implementations services at ACI Worldwide. Rao served as the head of analytics and insights at eBay's global risk, policy, and compliance organization; prior to eBay, he was the head of analytics at PayPal.

**Vantiv Inc.**, the second largest payment processor in the United States, has announced its agreement to acquire Moneris USA, the U.S. subsidiary of **Moneris Solutions Corporation**, which is a joint investment between BMO Financial Group and Royal Bank of Canada. The transaction is expected to cost US\$425 million and should close at the end of the year, subject to U.S. antitrust clearance and other conditions.



### Fast Fact

Fifty percent of U.S. consumers across all age groups are at least somewhat interested in **using an app to store gift card information** on their phone, with 59 percent preferring to use one app to store gift cards from multiple merchants.

Source: "2016 U.S. Prepaid Consumer Insights Study," First Data

# YOUR ETA: NOW

Cayan now has a  
75,000-customer base  
with the help of ETA.

ETA has helped us build our business over the past 15 years. From the business relationships and the advice we get from other members year-round, we've learned the inner workings of the industry and have seen the future. There really is no other resource for our industry like ETA.



Henry Helgeson, CEO and Co-Founder, Cayan

**ETA**  
ELECTRONIC TRANSACTIONS ASSOCIATION  
Advancing Payments Technology

ELECTRAN.ORG

Experience the value of ETA Membership and arrive at a greater level of success. Join today.

## Reflections on Advocacy

### ETA's year-end legislative and regulatory update

By Scott Talbott

**A**s the second session of the 114th Congress draws to its close, and the United States enters a lame-duck session in anticipation of a new president, ETA remains hard at work advocating for the interests of the payments technology industry.

On the legislative front, several new bills have been drafted pertaining to payments. ETA supports the bill introduced by Rep. Scott Tipton (R-Colorado) to exclude deposits of prepaid funds in FDIC-insured institutions from the definition of brokered deposits, and ETA takes a neutral position on the bill introduced by Reps. Jeb Hensarling (R-Texas) and Randy Neugebauer (R-Texas) to repeal the Durbin interchange restrictions. ETA will continue to press for passage of a single federal standard to address data breach before the end of the year. Additionally, we will continue the fight against Operation Choke Point, keeping the pressure up and using the revised ETA *Guidelines on Merchant and ISO Underwriting and Risk Monitoring* as an example of how best to reduce and eliminate fraud.

We've recently hosted several notable events, connecting key industry players with decisionmakers. On September 21, ETA hosted our annual executive fly-in in Washington, DC, sponsored by CAN Capital, to lobby members of Congress about issues facing the payments industry. Fifty ETA executives attended, and we met with 35 members of Congress as well as the Federal Trade Commission (FTC), Consumer Financial Protection Bureau (CFPB), Federal Reserve, and Treasury officials. On September 22, ETA hosted our inaugural FinTech Policy Day. Speakers included representatives from Intel, Visa, Amazon, American Express, Discover, Netspend, Wal-Mart, OnDeck, the U.S. Office of the Comptroller of the Currency, FTC, CFPB, and Hill staff. Deputy Whip Patrick McHenry (R-North Carolina) was a keynote and announced the introduction of his third fintech bill. We had more than 150 guests for this sold-out event, and we've already begun planning our 2017 FinTech Policy Day. Most recently, October 27 was ETA Policy Day, "The Future of Authentication," hosted at Google's DC office in partnership with the FIDO alliance. These and other imperative ETA events offer the opportunity for payments leaders to connect face-to-face with our industry's influencers to discuss priorities, champion progress, and shape the future of payments.

The Voice of Payments is our industry's most effective conduit for effecting positive progress, as federal regulators continue to press their agenda, which presents real threats to the payments



industry. There are numerous regulatory issues that ETA is actively monitoring and addressing with the CFPB. That agency has issued a proposed regulation to limit the use of predispute arbitration clauses. ETA submitted comments opposing the regulation last August. Our position is that arbitration is cheaper and faster, and garners a higher reward for consumers, than class-action lawsuits. The CFPB has also issued a proposal that would allow consumers to complete a survey and provide a narrative after receiving a company's response to their complaints to rate the company's response. The surveys and narratives will be posted on the CFPB's website. ETA will be filing comments opposing that proposal. ETA's position is that companies' reputations are at risk of being unfairly tarnished by such a process because consumers who are unhappy with or otherwise dissatisfied with a company's response will be far more likely to complete the survey than consumers who are satisfied with the response.

In addition, the CFPB has issued a notice of proposed rule-making in which it recommends significantly loosening the restrictions on its ability to make discretionary disclosures of confidential supervisory reports and other confidential information. ETA plans to file comments opposing the proposed changes to the rules. The CFPB's proposal to disclose confidential supervisory and other confidential information to foreign governmental authorities and non governmental entities is contrary to the language of the statute. Lastly, the CFPB issued its final rule for prepaid cards on October 5. The final rule dictates short and long form disclosures; numerous restrictions on overdraft, including requiring an ability to repay analysis; a 30-day waiting period; limitations on fees; and an opt-in requirement. ETA met with the CFPB and filed a comment letter opposing the prepaid regulation. We remain concerned about loss of access to prepaid cards for low- and moderate-income Americans; however, we will work to implement the regulation.

Beyond the CFPB issues, the FTC has initiated a number of enforcement actions against payments companies. ETA's guidelines have been helpful in shaping policymakers' thoughts about

the industry. ETA has updated the guidelines once and continuously asks if facts and circumstances have changed enough to warrant another update. Separately, ETA will file a letter urging the FTC not to make any changes in the Safeguards Rule, which requires financial institutions to implement programs to guard the privacy and security of their customers' information, following the rule's periodic review. And, in response to the FDIC's request for comments on its proposed guidance on third-party lending, ETA intends to file comments describing, among other things, the innovations fintech companies have brought to the lending market and how important online marketplace lending has become to the small business community.

### State Talks

ETA is focused on the increased attention from state regulators looking to enforce money transmitter laws, and we have been briefing state regulators on the intersection of the modern payments system and existing money transmitter laws. Maryland, Pennsylvania, Washington, and New York are among the states where we intend to offer comment on statutes or regulations.

Additionally, New York's Department of Financial Services (DFS) has issued regulations that require banks and money transmitters to tighten up their anti-money laundering programs by establishing Transaction Monitoring and Filtering Programs. The new rules go into effect Jan. 1, 2017. Beginning April 15, 2018, company boards or senior officers will have to submit annual certifications of the actions taken to ensure compliance with the new rules. And, the New York DFS has issued a proposed rule

that would require all banks and other financial institutions that the department regulates to implement cybersecurity programs to protect consumer and institution information from cyberattack. The rules are very prescriptive, and ETA intends to file comments in opposition.

In Washington State, ETA successfully lobbied the Department of Financial Institutions to halt enforcement of a new interpretation that treated payment processors as money transmitters until early 2017. We are also working with the department to amend existing law to create a more explicit exemption for payment processors from the money transmitter laws. The proposed change is being presented to the governor for review before being sent to the state legislature.

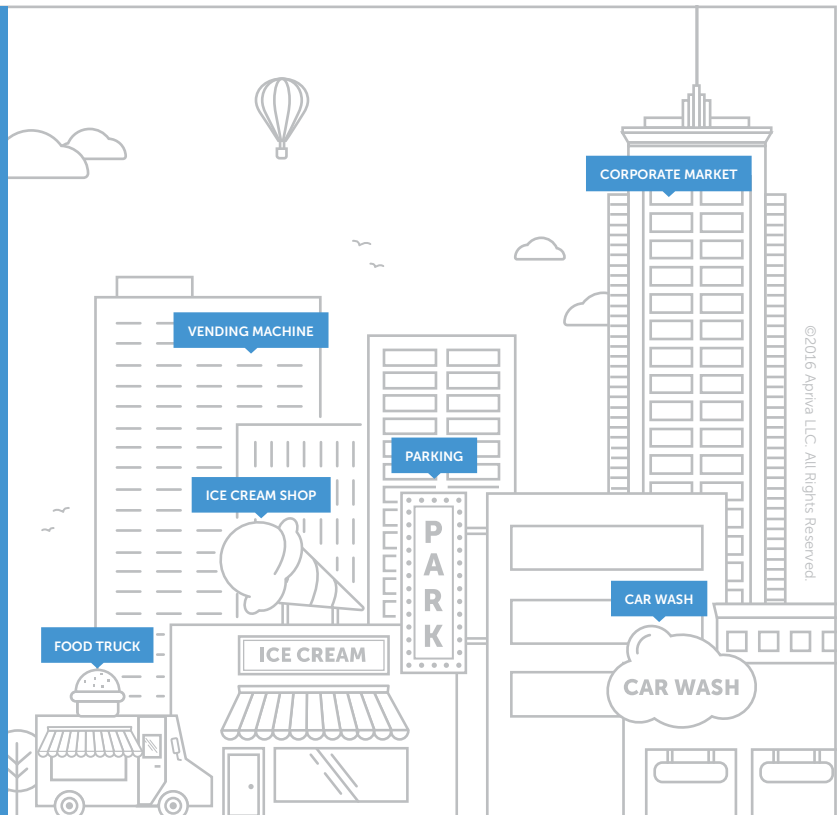
As you can see, ETA has been tireless in working to represent the best interests of our member companies, and we take seriously our role as the Voice of Payments™. In the coming year, we intend to do even more by expanding our political action committee, ETAPAC. During 2016 the ETAPAC has raised more than \$70,000 so far—a record—in contributions and pledges from 25 individual ETA executives and PACs. We have 67 percent participation by eligible ETA board officers, directors, and advisors, and 100 percent participation by the ETAPAC Board. We will continue to expand our advocacy efforts and focus on the federal and state legislative and regulatory issues that matter to payments professionals. **TT**

*Scott Talbott is senior vice president of government affairs for ETA. Reach him at [stalbott@electran.org](mailto:stalbott@electran.org) or 800/695.5509.*

## FREEDOM TO CHOOSE

With the largest support network in the industry, Apriva's POS solutions give companies of all sizes the freedom to choose the devices and processors that work best for their business. By connecting to all major wireless carriers, more than 35 payment processors, over 40 hardware providers, plus robust API/mobile integration, Apriva empowers your merchants to sell anything, anywhere.

Learn more at [Apriva.com/POS](http://Apriva.com/POS)  
877-277-0728





# Blurred Lines

By Ed McKinley

How payments facilitators are adding another method of merchant acquiring to the payments landscape

Once again, the payments industry finds itself gripped in the throes of change. It's happening as independent software vendors (ISVs) add payments to the bundles of business services they create to help retailers, nonprofits, and government agencies manage their enterprises. If an ISV becomes capable of offering all or most aspects of payment on its own and registers with the card brands to do so, it earns the formal title of "payments facilitator." When an ISV gets third-party help with providing payments, the ISV still looks like a payments facilitator to its merchants.

"Payments facilitator" seems to be the new buzzword in the industry," says Holli Targan, an attorney and partner at Jaffe Raitt Heuer & Weiss. She defines payments facilitators as aggregators, merchants of record, or master merchants that facilitate card acceptance by sponsoring and aggregating transactions for submerchants. Visa and MasterCard use the term "payments facilitator" in their rules, while American Express and Discover call them "payment service providers," she says.



Although the payments-facilitator phenomenon isn't exactly new, it's becoming more widespread and appears likely to keep expanding, according to Todd Ablowitz, president of Double Diamond Group LLC, a Colorado-based consulting firm. "We're in the first or second inning," he says of the movement. About 200 payments facilitators are operating in North America, and worldwide the figure stands at about 600, he estimates. "All of the major card brands, including Visa, MasterCard, American Express, and Discover, have welcomed the involvement of software vendors in the payments revenue stream by way of the payments facilitator model," he notes.

About 11,000 U.S.-based ISVs could benefit from the payments facilitator model, Double Diamond research indicates. The firm arrived at that figure by starting with its database of 23,000 ISVs actively selling in the United States and then subtracting any that don't receive payments and those that sell in the United States but have headquarters abroad. Of those 11,000 ISVs, 4,200 operate in the card-present market and have potential gross payment volume of \$787 billion; 6,300 are in the card-not-present market and have potential gross payment volume of \$772 billion.

"We expect that the payments-facilitator market, excluding PayPal, Square, and Stripe, will continue to double annually for at least two more years, with growth moderating in subsequent years to yield an average annual growth of more than 80 percent over the next five years," the Double Diamond research states.

Meanwhile, about 1,200 ISOs are listed with Visa, with most of the sales volume generated by the top 100, says Ablowitz's colleague, Rick Oglesby, a partner and head of product consulting at Double Diamond. Somewhere between 10,000 and 20,000 salespeople are working in the industry, with about 5,000 of them active, Oglesby says.

## Responding to a Need

Recognizing the proliferation of payments facilitators, ETA has created the *ETA Payment Facilitator Guidelines* to help members negotiate the intricacies of the business. "Payments facilitators present another segment emerging in the payments industry and demonstrate the opportunities for market changes in the ecosystem," notes Amy Zirkle, ETA director of industry affairs.

The organization also is planning a full day of programming dedicated to payments facilitation on May 11 at TRANSACT in Las Vegas. In addition, its TRANSACT Tech series of events is intended to engage leading-edge payments businesses, including payments facilitators, according to Del Baker Robertson, ETA vice president of strategic partnerships.

The growth of payments facilitators has apparently piqued Ablowitz's interest: His company recently finished a white paper on the subject; he helped prepare the ETA guidelines; and he publishes PaymentsFacilitator.com to disseminate news and

"PAYMENTS FACILITATORS PRESENT ANOTHER SEGMENT EMERGING IN THE PAYMENTS INDUSTRY AND DEMONSTRATE THE OPPORTUNITIES FOR MARKET CHANGES IN THE ECOSYSTEM."

— Amy Zirkle, ETA

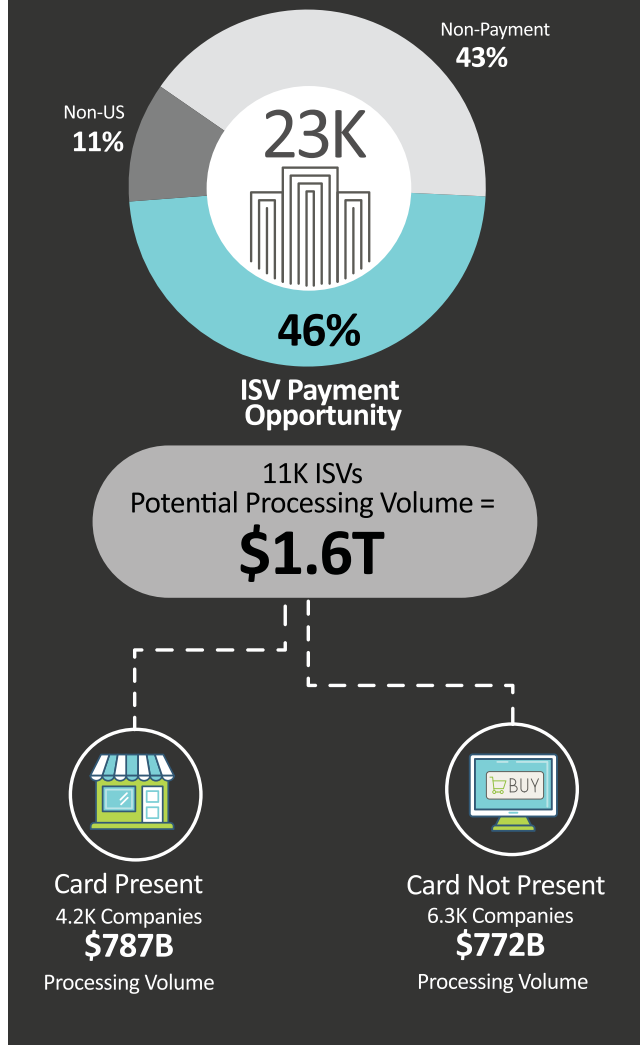
analysis. Ablowitz finds it helpful to view payments facilitators as belonging in either of two camps: wholesale or retail. Wholesale payments facilitators earn revenue from the transactions they enable and take on all or most of the risks and duties (such as underwriting and compliance) generally handled by ISOs and acquiring banks. Retail payments facilitators get third-party companies, such as WePay, Braintree, or Digitz, to help with the job of providing payments services, may or may not make money from the transaction services, and generally avoid the potential downside. One might think of the latter as looking like payments facilitators without really being payments facilitators.

Oglesby describes payments facilitators this way: "Being a payments facilitator is a way of enabling an ISV to be ISO-like and earn these revenue streams as though they were an ISO, when in reality they are a merchant." In effect, payments facilitators' customers become submerchants in the payments landscape.

## Function and Fulfillment

Slippery definitions aside, payments were usually an afterthought back in the days when ISVs began offering their wares to customers and including payments in the bundles of capabilities they create, says Laura Wagner, CEO of

There are 23,000 business-to-business software-as-a-service companies generating \$32.8B annually. Nearly half are in the ISV addressable payments market, making them ideal candidates to become payments facilitators.



Source: Double Diamond Research

Digitals. Hardly anyone would skip payments now, she adds.

In fact, some ISVs that become facilitators have switched much of their focus to the payments element of their offerings, notes Oglesby. Some go so far as to make payments their main source of revenue and provide their software to merchants at little or no cost, he says. In such cases, the company might charge a premium on the transaction, boosting the fee to 5 or 6 cents from the usual 2 or 3 cents, for example. But, it's still a reasonable deal, he says. Those higher fees can make sense, Oglesby maintains, because when an ISV charges a merchant only when a transaction occurs, the ISV is also charging only when its software comes into play.

It's also reasonable to view the payments facilitator business as already quite large by considering such companies as Adyen, PayPal, Stripe, Shopify, and Square as members of the category, Oglesby explains. PayPal is approaching \$300

billion in processing volume, while Stripe and Square are both closing in on \$50 billion in volume, he says.

Vantiv is enlarging the market, too. In 2010, the company worked with Visa and MasterCard to write the rules for payment facilitation in the United States and called their finished product the "payment service provider model." Vantiv even patented the word "PayFac" for the category. That's all according to Matt Downs, ETA CPP, head of channel and business development for Vantiv Integrated Payments, which was formed this year by bringing together the company's Mercury and Element subsidiaries.

These days, Vantiv is working with "north of a 1,000" ISVs and claims that more than 80 percent of the payments facilitators registered in North America are its clients. Downs notes that the company offers programs for ISVs at any stage in their progress toward becoming payments facilitators. He says that with "turnkey" offerings, "all they have to do is code onto our platform, and we do the rest." Other programs would accommodate ISVs more sophisticated in the payments business. "The degree they want to build it up and support it is really on a company-to-company basis," he says of ISVs and payments facilitation. Some begin with a turnkey program and grow. Others elect to start as a full-blown PayFac and subsequently decide to back off to a more moderate degree of independence.

Vantiv claims to help ISVs improve the customer experience, and Downs provides the example of "staged underwriting." Vantiv provides access to the infrastructure for the process. For example, suppose that a new merchant wants immediate access to an accounting package that includes payments. The ISV can collect 10 or so data points and make a quick decision to enable the merchant to begin a small number of transactions almost immediately. As the ISV gets to know the merchant, it can grant higher volume.

To speed up that process of getting acquainted, Vantiv offers dynamic funding that updates a merchant's underwriting file with every transaction—instead of the old way of waiting for an evaluation that may have occurred only quarterly, Downs says.

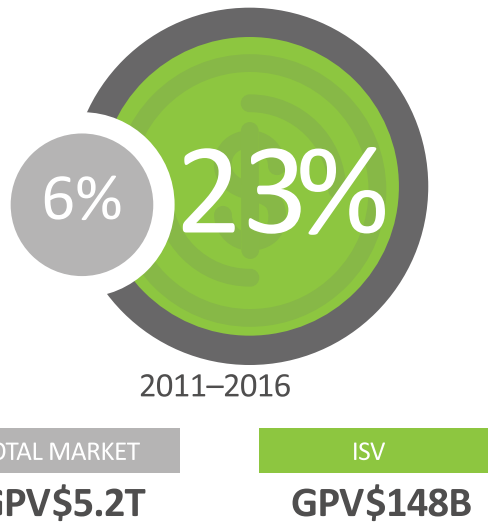
Those advantages have contributed to the prodigious growth of ISVs in payments, but that success does not come solely at the expense of ISOs that have traditionally promoted transaction services to merchants, says the ETA's Zirkle. That's due to a lack of overlap—some verticals fit more naturally into the world of ISOs, while others more closely match the ISV scene. "ISOs will continue to exist—and continue to serve larger merchants," she says. "Payment facilitators tend to serve smaller merchants and merchants in merging channels."

### The Right Fit

ISOs hold their own with the types of customers they have courted for decades, such as retailers, restaurants, and salons, observers agree. Proprietors of many of those businesses have become comfortable viewing payments and business-oriented software as separate, says Downs. What's more, many merchants in those segments just don't need the services ISVs



**The growth in ISV-derived gross processing volume (GPV) is outpacing growth in the retail-centric acquiring industry by nearly four times.**



Source: Double Diamond Research

provide because those merchants seldom or never receive electronic payments, he maintains.

Conversely, entities that seem to mesh with ISVs, according to Wagner, include utility companies, units of government, and nonprofits. ISOs simply haven't been contacting many of those entities. Ablowitz suggests that other types of businesses that represent opportunities for ISVs are hospitality, digital commerce, bill payment services, and fitness. ISVs do well in market segments where cash is still dominant and in segments that aren't always thought of as merchants, such as apartment rentals or Airbnb, according to Downs. And Oglesby says that, unlike ISOs, ISVs can often profit from one-time events, health-care providers, and new types of businesses.

One example of a new type of business where ISVs can hold sway is Uber, explains Oglesby. Like so many new businesses, Uber cannibalizes more-established competitors to some degree—in this case the taxi business—but accrues much of its growth by expanding the market. Uber, for example, will pick up your groceries, while a taxi cab driver probably won't. A Google search for the word "uber" combined with other words or phrases, such as "karate" or "medical marijuana," yields a host of new businesses, he notes. Some of those new businesses offer lots of advantages, like the "uber pizza" restaurants that keep customers' favorite toppings on file.

New businesses are proliferating because of the apps consumers download onto their mobile devices, says Downs. People are becoming accustomed to using their phones to order dinner, pay in advance for a movie, or remotely monitor the security systems in their homes, he explains.

But even though ISVs don't threaten ISOs with extinction, analysts still urge the latter to take precautions. "Differentiate or die," Ablowitz advises ISOs.

Agreeing, Downs contends that "the days of selling stand-alone solutions are going to be challenged." Merchants are simply coming to expect lots of features, Downs concludes.

Attempting to offer value-added products and services can lead ISOs to promote business-oriented software or other options in addition to payments, both Ablowitz and Downs maintain. What's more, Oglesby points out that ISOs can actually become ISVs by creating programming. For years, industry observers have been encouraging ISOs to include value-added products like software to the list of offerings they promote to merchants. Thus, ISOs can differentiate themselves from competing ISOs while also rivaling ISVs in the breadth of their wares. ISOs that shy away from becoming programmers can seek opportunities to distribute software for ISVs that lack merchant contacts, Oglesby suggests. "Not everybody was born to [write] code," Downs humorously suggests, and observers agree that some ISVs lack sales expertise and would benefit from working with ISOs that have extensive merchant contacts.

But even as more ISOs come to resemble ISVs, Downs suggests that not all ISVs will become payments facilitators. In some verticals, the advantages of controlling payments just aren't great enough to justify the effort and expense, he says. That would include verticals that need software to run operations, not to sell products. That's why he typically advises anyone in payments to find hardware and software and sell it to increase margins. "Everyone's got to pick up a piece of software and say, 'How can I translate this into value of merchants in a particular vertical?'"

Downs' own company is heeding that advice. The payments scene is becoming more complicated as Vantiv becomes somewhat of an ISV itself. The company recently announced a partnership with Verifone to introduce the Verifone Carbon Commerce Platform as part of Vantiv SmartFit Solutions. The product operates as a POS device that includes order and inventory management software, tools for online analytics and reporting, and a gift card program that the companies say many small business owners could not otherwise afford.

Perhaps the onslaught of payments facilitation—like so many disruptions—is blurring the lines among entities in the payments business. If that's the case, however, it seems certain that companies will find ways to differentiate and thus create another wave of disruption. In payments, everything changes. **TT**

*Ed McKinley is a contributing writer to Transaction Trends. Reach him at [edmckinley773@yahoo.com](mailto:edmckinley773@yahoo.com).*

**BONUS CONTENT:** Looking to become a payments facilitator? Learn more about the ETA Payment Facilitator Guidelines and download a copy at [www.electran.org/pf](http://www.electran.org/pf).



How financial institutions are extending  
data access to third parties and payments  
businesses to keep pace with  
fintech innovation

By Christine Umbrell

# 'OPEN' for BUSINESS

One of the hot topics swirling around today's banking industry is the discussion of banking application programming interfaces. APIs are seen by some as an essential tool for banks competing in a mobile-focused economy. They have the potential to change the way banks share information with fintechs and payments businesses, allowing for faster development of innovative products and services integrated with data from financial institutions. But what exactly are APIs, and how will this transformation happen?

An API serves as a "middleman" between a programmer and an application: The API accepts requests and returns the requested data. The API also informs programmers about what they are allowed to request and how to request it.

"There is a movement at banks toward using APIs to allow for improved interfaces between clients and banks' back-office systems," says Nancy Atkinson, a senior analyst with Aite Group. "Banks are looking at this trend and asking, 'What are APIs, and how can we use them to modernize our technology infrastructure and provide greater transparency to our clients?'"

"APIs enable one piece of software to talk to another piece of software," says Kristin Moyer, research vice president and distinguished analyst in Gartner's banking/investment services practice. "APIs provide access to data, algorithms, transactions, business processes, and application capabilities. APIs are most

commonly used by mobile apps, third-party websites, and, more recently, chat bots and digital assistants."

In the banking industry, APIs enable open banking—a platform business approach to facilitating the exchange or creation of new goods, services, and social currency, says Moyer. "We believe future value creation will come more from sharing, providing, and leveraging key assets than protecting them." Open banking does this by making various data and other business information available to employees, third-party developers, fintechs, vendors, and other partners, says Moyer.

"Banking APIs essentially provide controlled programmatic access to select customer and account information and banking capabilities," adds Rich Urban, president of IFX Forum Inc., an international nonprofit industry association whose mission is to develop and promote the adoption of its open, interoperable standard for financial data exchange. "Open banking APIs



**Earn ETA CPP Continuing Education Credits** Read this article, then visit <http://www.electran.org/eta-cpp-quiz-api> to test your knowledge and earn 2 ETA CPP CE credits per quiz!

refers to broadening data access based on open standards or a public interface.”

There are three distinct categories of open banking APIs, says Moyer: internal APIs, used by employees inside the bank; private APIs, used by customers and partners of the bank; and public APIs, used by third-party developers and others outside the bank. As an example, Moyer cites an API that brings together current account transactions and credit card transactions. “This could be used internally at the bank, by employees,” she says. “It could be shared with customers, via a private API, so that they can log into their online banking application to see current account transactions and credit card transactions in one place. It could also be shared with third-party developers or other business ecosystems outside the bank so that they could build mobile apps that help customers better manage their finances.”

### Leveraging APIs at Financial Institutions

While the percentage of banks that are leveraging APIs is currently very low in the United States, the trend is taking hold. “Banks are exploring APIs. There are many internal proof-of-concept trials going on, and limited offerings being tested” at

as its clients—also has begun using APIs to allow its tech-savvy clients to create their own user experiences, says Atkinson.

In Europe, several banks are leveraging open APIs to provide access to transactions, algorithms, data, and other business services, says Moyer, citing BBVA, Fidor Bank, and Barclays, among others. “And some banks are providing APIs that are enabling fintechs to build their own bank,” she says. For example, Fidor TecS, the technology division of Fidor Group, has an API layer called fidorOS. “It is middleware built on top of a local core banking application—Bancos—with Ruby/Ruby on Rails using MySQL,” explains Moyer. Fidor TecS performs the functions of a banking system, but can run on top of any existing core banking application. “Third parties can use the Financial Open eXchange Initiative (FOXI) to create applications within fidorOS.” Fidor TecS also licenses fidorOS as a white-label solution, says Moyer.

The U.S. banking industry is three to five years behind other developed regions of the world when it comes to APIs. “Europe has a number of regulatory-driven directives—for example, PSD2 [Revised Payment Service Directive], and the Open Banking Standard—that are requiring banks to use APIs to share things like customer data, transaction data, and payment initiation,” says Moyer. Some European banks “are using APIs to enable new mobile apps, digital products, and business models.” India also is ahead of the United States in this area: “The National Payments Corporation of India created the Unified Payment Interface (UPI), which enables things like in-app payments and proximity payments,” Moyer says.

In the United States, APIs have the potential to revolutionize the banking industry in several ways. “We have seen banks reduce the time and cost to market for new business capabilities by 50 to 90 percent,” says Moyer. “Some banks that have used APIs as a new business channel have increased their net revenue growth by up to 30 percent year-over-year.”

API development also may improve the consumer banking experience, and enable banks to innovate more quickly. “We have seen banks bring new mobile apps and digital products to market that make banking easier, more transparent, and more convenient for customers,” says Moyer. APIs can enable a rapid cycle of innovation, which can allow banks to experiment with new services and programs, she says—“many of which may fail, but some of which will create value in new ways for customers and banks.”

### Banks as ‘Marketplaces’

The growing demand for APIs stems from a number of factors, says Urban. For example, bank customers are seeking creative solutions, such as mobile apps, that require financial institutions to collaborate with third-party payment providers. To cater to that demand, the banks themselves are seeking to reduce the risk of current market practices. Urban also cites the “expectations of the millennial generation” to conduct mobile transactions as a reason some banks are experimenting with APIs.

Open banking APIs allow for “user experience on steroids,”

OPEN BANKING APIS ALLOW FOR “USER EXPERIENCE ON STEROIDS,” GRANTING APPROVED CLIENTS **THE POWER TO ACCESS THE BANKING SERVICES AS THEY CHOOSE** AND CUSTOMIZE THEIR BANKING INTERACTIONS.

U.S. banks today, says Urban. “They’re trying to figure out what the system boundaries need to be.”

U.S. banks like Capital One and E\*TRADE are leading these efforts, using APIs to create new digital products and services, integrate more deeply with customers, and enable new types of customer experiences, says Moyer. Elavon, a processor backed by US Bank, has an API that “enables developers to write a point-of-sale application that integrates with its Converge payment platform,” says Moyer.

Atkinson notes that BBVA Compass currently offers real-time payments through Dwolla by providing the bank’s clients with single sign-on to Dwolla using open APIs. Silicon Valley Bank—a California financial institution with tech companies

says Atkinson, granting approved clients the power to access the banking services as they choose and customize their banking interactions.

Moyer says leveraging the technology can help banks become “a marketplace of solutions”—one that offers traditional bank products and services, like deposits, loans, and payments, as well as “solutions that ecosystem partners have built using a bank’s APIs,” such as apps and new digital products and services. APIs also can be used to integrate with alternative payments solutions, such as blockchain/metacoin platforms, as well as loyalty schemes, says Moyer. “A banking customer could log into their online banking system and see current account transactions, credit card transactions, and Bitcoin transactions, all in one place.”

Having a marketplace of solutions may help banks remain relevant, because it offers one-stop shopping, where customers could “visit” a bank with a marketplace to get all their needs met, says Moyer. “Today, they go to multiple banks and also to fintechs. The risk is that banks become relegated to the back-end, holding all the cost and all the risk, while fintechs mainly control the front-end relationship.” The marketplace model has the potential to help banks remain at the forefront with customers.

In addition, the marketplace model may inspire new revenue streams. “Banks can take a revenue share of ecosystem partner solution sales,” says Moyer.

Atkinson advises banks to take a page from Amazon’s playbook. Just as Amazon progressed beyond traditional ful-

fillment to allow third parties to sell products to a larger audience—and take a cut of the sales in the process—banks can offer specific financial services that consumers can purchase through the portal of the bank. “The bank does not have to build or maintain these extra services, just offer them,” via API development, says Atkinson.

The possibilities for new digital products that may be developed using APIs at financial institutions are almost endless, according to Moyer. Personal data banks, digital identity services, trust brokers, and reverse auctions are a sample of products that could be developed—with or without the assistance of third-party vendors.

Payments professionals in particular stand to benefit from the proliferation of API technology as well. Moyer advises innovative payments companies to “provide APIs that make it easier for banks to use your products and services; create new digital products for banks that can be accessed via APIs—for example, new data and identity services; and use APIs from banks to create new mobile apps, digital products, and business models.” The most successful solutions will be scalable, reliable, secure, and compliant, says Moyer.

### Growing Pains

As with any evolution, the movement toward open banking APIs comes with some challenges that must be overcome if banks and their partners hope to benefit from the technology. Risk management is at the top of that list. “Banks should adopt a risk-based approach to securing APIs, taking into account

# eProcessing Network

INTRODUCES

## Premier Plus

- Our Secure EMV and MSR Bluetooth Card Reader
- Supports iOS and Android

800-296-4810

eProcessingNetwork.com



eCommerce



Bill Pay



QuickBooks



Texting



Level 3



CDM



Inventory



the APIs' business value, sensitivity, criticality, and the consequence of compromise," says Moyer. Institutions will benefit from establishing responsibilities for API security "that encompass developers, enterprise security, and digital business stakeholders."

Urban notes the importance of establishing system boundaries. When data is exposed to external partners and applications, it is necessary to establish levels of trust and security measures to ensure proper authorization and access to the data, he says. For example, a bank providing APIs to its corporate clients over a private network has a different set of boundaries than it does when providing APIs to aggregators serving thousands of individual clients. "In the first case, there is really only one boundary for the data to cross: from bank to corporate client over a trusted connection," says Urban. "In the latter case, the bank will have to establish risk and liability agreements with the aggregator; will have to secure access to a select set of customer data for that aggregator; and must consider that the connections to the aggregator and its clients may be less secure and that the data may be in transit 'in the cloud.'"

Regarding security concerns, Urban says the risks involved in seeking financial data without involving APIs are significant: "The lack of standardized APIs has led to the broad use of unsafe practices by consumers—practices that create risk for users and financial institutions," says Urban. His organization, IFX Forum, is currently working to set the direction for a standardization effort. "The lack of APIs is causing consumers to use unsafe alternatives to gain access to their data, including sharing their credentials with aggregators and other third parties whose security practices are unproven."

In addition to security concerns, "culture" is another area that must evolve before there can be widespread acceptance of APIs within the banking world. "Banks have historically focused on protecting business services like data," says Moyer. "But future value creation is going to come more from sharing business services than protecting them. APIs make this possible, but it can be difficult to get the bank to think and act differently about creating value in new ways." Also significant is the operational risk, in terms of security, integration, regulatory compliance, and reputation risk, says Moyer.

## Dwolla's Take on APIs and the Banking Industry

One of the most popular sessions at ETA's Strategic Leadership Forum in October was a keynote address by Ben Milne, Dwolla founder and CEO. Dwolla, a digital payment network that allows users to build applications that facilitate bank transfers, manage customers, and instantly verify bank accounts, is a leading innovator in the API space. Here, Milne discusses how APIs add value to financial institutions, and how APIs are being used to connect developers with banks.

### **Q: How has Dwolla leveraged API technology in connection with banks to provide innovative services?**

**Milne:** Our customers access the banking infrastructure through Dwolla, which is a set of APIs. If they are using our branded tools or our APIs to move money, they are using the API. The tools just sit in front of the API. A big part of the value that Dwolla provides is that we've made the banking infrastructure and bank transfers easy for developers to leverage and for businesses to integrate into their software applications.

Those companies that are building software that helps customers move



Milne at the 2016 ETA SLF

money and access the banking system are building great end-user experiences and technologies that connect to banks. Abe.ai, Current, RentMonitor, GOAT, and Get My Boat are good examples of this. All require traditional banking services, but need an API to move money between two U.S. banks or credit unions.

### **Q: Are these "open-source" APIs, and what should payments professionals know specifically?**

**Dwolla:** Most APIs for payments aren't open-source but are actually hosted by a service provider. The APIs may be served through open-source libraries. The benefits those libraries provide are ease of use for developers and a reduction in the investment required from a business to get their software into production.

Most marketed "open APIs" unfortunately aren't open. They are actually closed-off, permission-only systems. The best ones

Atkinson says the governance model for APIs with financial institutions is in flux. “Banks won’t let just anyone see all of their data,” she says, because doing so is against regulations and risks their reputation. “Open APIs may enable corporations to gather data—but they also allow clients to move their banking relationship very quickly.” This may alarm some banks, but “you can’t be that protectionist anymore. You need to have value-added services others don’t—and APIs can help with that.” Setting clear guidelines regarding the circumstances under which banks will allow other entities to access their data is a “must,” says Atkinson.

Moyer points to yet another potential barrier: monetization. “It is hard to get monetization right. Most monetization will come through incremental revenue for existing products at first. Over time, APIs can enable entirely new digital products, like digital identity services and personal data banks,” she says, adding that it can take time for banks to achieve a return on investment for most API-enabled initiatives. “APIs are a journey, not a destination,” says Moyer.

## The Start of Something Big

U.S. consumers are demanding access to their financial data, and APIs

are one of the tools banks can leverage to create innovative solutions. “It’s a cultural change to open up beyond traditional boundaries, but it’s also going to be a survival imperative,” says Anita Brady, current board chair of IFX Forum.

Atkinson believes open APIs will become a more significant aspect of financial institution offerings in five years. Considering all of the possibilities that emerge when banks allow access via APIs, it is clear this trend is here to stay. It is likely that this technology will become a new vector of competition among banks. Those financial institutions that become educated on APIs and partner with vetted fintech companies and others to offer innovative products and services stand to reap the benefits of early action.

“This is just the beginning,” says Moyer. “APIs and open banking will change the way banks create value in the future. What it means to be a bank will look very different in five to 10 years than it does today.” **TT**

---

*Christine Umbrell is editorial/production associate and contributing writing to Transaction Trends. Reach her at [cumbrell@contentcommunicators.com](mailto:cumbrell@contentcommunicators.com).*

make onboarding easy, helping open new revenue streams for banks.

When the customers—anyone digesting API services—find the right APIs to use, the two become an incredibly efficient way for banks to onboard new customers and expose those customers to additional services from the bank.

At Dwolla, we can help onboard thousands of customers per day to a partner financial institution. Getting that many people to walk into a branch is really expensive.

The bank system is harder than it should be to use, and we’re helping to lower that barrier for our partners. We’re far from done.

**Q: How are some banks today offering APIs to fintech/payments businesses, and how is this trend expected to evolve?**

**Milne:** Some banks have an open way of thinking by default. They want to build the next great digital bank for customers who are digital first and branch second. There are more and more of these banks getting started everyday, building new platforms.

Capital One has [been a leader in this area] with its digital and analytics initiatives, and

a number of financial institutions are taking the hint.

The trend is that more and more banks will continue to build digital platforms, and we’ll see more regulatory bodies think about how they can help it along. PSD2 in Europe is thematically similar in that the regulatory body is promoting collaboration and consumers being in charge of their information.

By financial institutions giving consumers control, they are inherently opening themselves up to more ways of doing business through fintech providers who may access that information on behalf of the account holder.

**Q: What are the security concerns related to APIs, and how can they be alleviated?**

**Milne:** The security concerns of an API are similar to that of any trusted service: confidentiality, integrity, and availability of the service and data.

An API must support strong cryptography to deliver confidentiality to its consumers, including protective configuration and guidance for safe implementation. The integrity of messages and data is supported by encryption but further advanced

by the signing of messages to ensure they are not forged. Lastly, an API needs to be available as delivered by design and configuration. This is achieved by a combination of robust services and endpoints, load balancing, volumetric DDoS protection, and, where necessary, rate limiting and management of abuse.

On top of this foundation, standards—both the lack of standards and the onset of standards—pose a considerable risk to the evolution and security of APIs. APIs, by their nature, are meant to evolve and meet the pace of technology and market demands. Their evolution will almost assuredly outstrip any attempt to standardize API security in general. At the same time, the lack of standards creates obvious concerns.

There is going to be a balancing act for regulators and providers as they attempt to manage the freedom to select the best security practices at the time without holding them back by mandating old standards that will be outdated quickly. For the time being, [the best approach is to] follow best practices, stay up to date, and hire good people. I’d highly recommend taking part in local and industry security groups. **TT**



Hayden at the 2016 ETA SLF



# Cyber Security in a Dangerous Time

Gen. Michael Hayden explains why protecting the domain is still so hard

One of the foremost experts in the United States on cyber security, Gen. Michael Hayden has more than 40 years of experience as a military leader. He's a retired four-star general, and he served as the director of the Central Intelligence Agency and as the director of the National Security Agency (NSA) during a time of tumultuous world events.

At the 2016 ETA Strategic Leadership Forum in October, Hayden leveraged that experience into a frank discussion about the state of cyber crime, including the current political landscape, the global threat of terrorism, and how private-

sector businesses will have a front-row seat in shaping the future of cyber security.

## Who's Doing What

In his work at the NSA, Hayden found himself trying to convey to savvy audiences the paradoxical and profound effect the advent of the internet and digital technology has had on society and on every aspect of human life. While it has empowered a world, it has also introduced unprecedented kinds of insecurities and risks.

"It's the biggest deal we've experienced since the last great



age of globalization,” he said. “It’s the biggest thing our species has experienced since the European discovery of the Western Hemisphere and the voyages—the discovery that brought the world together.”

The sea voyages drew together civilizations that were developing autonomously and created the greatest leap in human learning and advancement, along with epidemics, global slavery, and other threats to society, Hayden argued. Similarly, our current age of digital globalization has introduced both “nourishing” and “poisonous” effects on society—data theft among them.

“It is such a big deal that your armed forces, your Department of Defense (DoD), now describes cyber as a domain,” along with land, sea, air, and space. English translation? It’s a location that our military fights for and protects. “This is a bigger deal than even the best of us truly appreciate. It is a whole new domain where you and I are now existing, where our ancestors never existed before,” he said.

But the cyber domain is distinctively different than the other spaces because it is manmade. It started out as a DoD project with the goal of moving large amounts of data quickly and easily to a few known entities, including federal labs and top universities such as Stanford and MIT. Security concerns didn’t factor into the initial project’s work, Hayden explained. The original architectural principle—large amounts of data delivered to a limited number of known and trusted entities—remains the principle of today’s internet, which has a seemingly limitless number of entities, most of which are unknown and untrusted. That, he said, is the fundamental issue of cyber security, and it only grows more serious as more people become connected.

Five years ago, a “cyber attack” primarily consisted of someone stealing another’s information, be it a “PIN number, credit card number, negotiating position, intellectual property, embarrassing emails, whatever,” said Hayden. Now,

security experts are seeing more dangerous and sophisticated activity, including data corruption, network denials, and physical destruction.

“The posterchild for [physical destruction] is something called Stuxnet, which was an attack on the Iranian nuclear facility at Natanz,” Hayden explained. “Someone, almost certainly a nation-state, used a weapon comprised of ones and zeros to destroy—during a time of peace—what another nation could only describe as ‘critical infrastructure.’”

Hayden categorized the perpetrators of these more sophisticated activities as nation-states, criminal gangs, and hacktivists—activists such as Anonymous and LulzSec. “I think the ones [payments professionals are] most focused on are criminal gangs,” he said. “You’re where the money is, so that’s where they go. But, I don’t think you’re immune from the others,” he said, adding that at one point Iran conducted a massive distributed denial-of-service attack against a series of American banks, including Bank of America, Wells Fargo, JP Morgan Chase, and others.

### Fighting Back

After explaining the details behind a series of headline-making cyber attacks around the world, Hayden discussed the challenges of fighting cyber warfare. In the case of “weaponizing” the digital space, he entertained the notion that a less “modernized” infrastructure could be immune, citing the Dec. 23, 2015, Russian attack on the power grid in Crimea and the Ukraine.

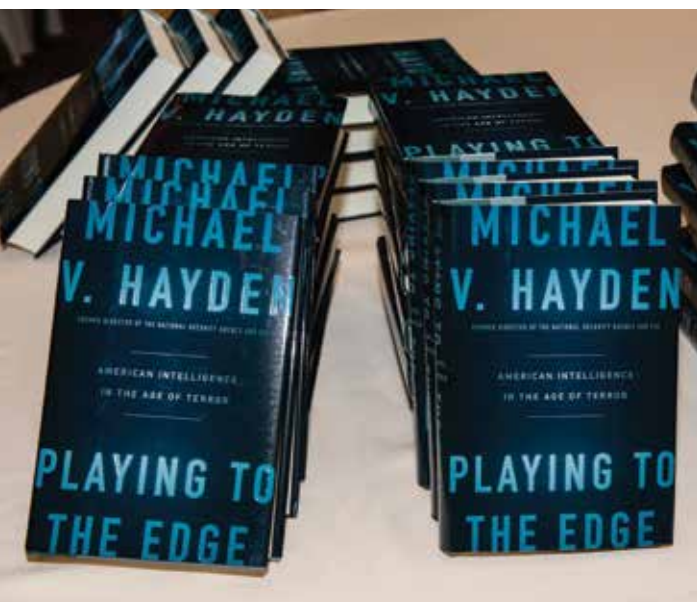
“It could’ve been worse. Most of the Ukrainian grid is still analog, and only the portion that was digitized went down,” he said. “Not very comforting, speaking to the citizens of a nation [that has] an entirely digitized national grid, and who are right now creating a smart grid so that all parts of the grid can talk to one another. . . . Actually, it’s a great way to govern the grid. It just makes it very, very vulnerable.”

So what is the U.S. government doing to protect the cyber domain and its citizens? “Not as much as you would think,” Hayden said. And the reason is more about civil liberties and less about political dysfunction. As a nation, Americans have yet to decide how to balance their right to privacy with government protection.

“Let me put it another way: You, personally and corporately, are going to have to be more responsible for your safety [in cyber space] than you have been required to be responsible for your safety since the closing of the American Frontier in the 1880s,” he said.

Still, the government is taking some action, including imposing economic sanctions against countries doing wrong. The Department of Homeland Security also has statutory responsibility to defend critical infrastructure, Hayden pointed out. But unless the attacks are “so vile, so big, so important that the Department of Defense” has to respond, then the private sector is “on its own” to defend against attacks.

“The instinct of our government has been—in the cyber domain as in physical space—that the main body was the government. . . . We may have that wrong. It may actually be



in the cyber domain, the main body for American defense is the private sector, not the government, and the government, then, should conform its movements to the movements of the main body, rather than the other way around.”

Need an example to his rationale? The lawsuit between Apple and the FBI last year, after the agency demanded Apple create a “backdoor” to its encryption code so that investigators could access the iPhone used by Syed Farook, who carried out the mass shooting in San Bernadino, California. Hayden, along with other prominent defense officials and security experts, sided with Apple because they believed that the good that could be gained was far outweighed by the security fallout that would have resulted from “punching a hole into the [encryption] system.”

With cyber domain still evolving, Hayden also pondered influencers, rules, and regulations, especially if we see government conforming to the movements of the private sector. How will laws be adjusted to accommodate the new realities and opportunities provided by technology? “When it comes to the 21st century definition of privacy and what constitutes a reasonable expectation of privacy, [Mark Zuckerberg] is going to have more influence over where we land than the Congress of the United States,” said Hayden. In essence, he expects political and commercial structures to adapt because the technology is so transformative to society that it cannot be denied.

### Risk Management

To conclude his discussion, Hayden offered a modernized view of the classic risk equation for the cyber domain. Vul-

nerability reduction—passwords, firewalls, good systems hygiene, and so forth—if executed perfectly, prevents about 80 percent of hackers, he said. While still necessary, it alone isn’t enough. Current cyber security demands “presumption” of breach and response.

“The difference between an A and an F player in consequence management is the time between flash and bang, the time between penetration and discovery. And, frankly, for all of American industry—not yours, but for all of American industry—that time between flash and bang is routinely measured in months, which is really bad.”

While difficult, accepting that hackers are and will get into a network is critical, Hayden added. “You need to be able to fight your network. Protect your more precious data more tightly, be able to detect when you’re penetrated, be able to reject the penetration, but it’s more of an active combat scene rather than deep moat, high walls,” he said.

In the future, cyber threat intelligence will be at the core of cyber security efforts, according to the Hayden. These private-sector companies that perform web crawling, port scanning, chat room monitoring, and more provide clients with actionable threat warnings. Cyber insurance also may help elevate the level of positive, proactive behaviors by American businesses, as well, because it rewards good network security with a more favorable rate. “Rather than have the government come into your offices with a whistle and a cap and a clipboard, and check [if] you’re complying with government regulations,” he argued, “this is a business model that actually would animate a lot of American industry to go for better cyber insurance because of raw return on investment.” **TT**

**USAePAY**  
Smarter Solutions For Secure Payments

- Free Tokenization
- Retail
- ACH Check
- E-commerce
- Developer Tools
- Mobile
- Fraud Tools
- Mail/Telephone order

NEAA 2017 - BOSTON  
January 31- February 2

USAePAY  
Established 1998

USAePay.com 866.490.0042

f t in i

# Glimmers of Hope?

The Eleventh Circuit nudges Operation Choke Point toward a more proportional remedy

By Edward A. Marshall

For the past several years, payment processors and ISOs have seldom received good news about Operation Choke Point—the moniker used to describe the pursuit of the payments industry by organizations such as the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) for the untoward acts of the merchants the industry serves. The arc of enforcement actions seemed to be accelerating in the wrong direction, with a trajectory of more litigation and the pursuit of increasingly draconian remedies.

Indeed, processors and ISOs went from being sources of information for government actors pursuing businesses engaged in consumer fraud to targets themselves. The FTC and the CFPB began to seek contempt sanctions against processors that allowed *their* contractually established reserve funds to be used to satisfy consumer chargebacks. The government organizations claimed those processor dollars were subject to freezes imposed on the target merchant's assets. And then, processors and ISOs (along with individual principals) began to be named as defendants in cases alleging unfair and deceptive practices against merchant co-defendants. The government sought to hold them liable, not only for the revenues associated with “bad apple” merchants but also for the *entirety* of the consumer harm perpetrated by their merchant customers.

Such initiatives by the FTC and CFPB show little signs of abating. Even from the vantage point of industry advocates, it is difficult to dispute that *some* boarding, underwriting, and risk-monitoring practices—at least at the peripheries of the acquiring world—are appropriately subject to criticism and disruption by regulators. But what has become increasingly difficult to accept is the severity of the remedies the government is seeking to extract from processors, ISOs, and their (individual) principals



when merchants seeking to engage in deceptive consumer conduct exploit those practices. Often, the relief pursued by the regulators is disconnected from the limited role acquirers played in the allegedly improper conduct and grossly disproportionate to the relatively small fraction of transaction value that went to the processor or ISO in the form of processing fees or residuals (as opposed to the bulk of the transaction proceeds that went to the merchant).

The FTC's case against Universal Processing Services of Wisconsin LLC (UPS), which it initiated in a Florida federal court, underscored both the dangers of litigation and the extent to which a finding of liability could result in a shockingly disproportionate result. See *FTC v. WV Universal Mgmt. LLC, et al.*, Civil Action No. 6:12-cv-1618 (M.D. Fla. filed 2012). There, the FTC alleged that a telemarketing scheme, known as “Treasure Your Success,” was able to gain and maintain access to

the payments grid through UPS despite the presence of multiple red flags. Warning signals included a high-risk business model, extremely high chargeback ratios, 20 percent reserves, and failure to abide by internal UPS policies. The FTC contended that UPS provided “substantial assistance” to the telemarketers while knowing or “consciously avoid[ed] knowing” of multiple violations of the Telemarketing Sales Rule (TSR), 16 C.F.R. Part 310, which is itself a violation of the Rule. Based on those allegations, the FTC sought relief under Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), which authorizes the equitable relief, including disgorgement and restitution, and Section 19 of the FTC Act, 15 U.S.C. § 57(b), which authorizes a court to redress consumer injury.

Several defendants, including the telemarketers themselves, settled quickly and for either no money or relatively minuscule sums. But UPS chose to fight, claiming that the individual who facilitated the boarding of the telemarket-

ers and allegedly turned a blind eye to the red flags was acting in violation of company policy. Ultimately (and given the referenced individual's leadership role within the company, perhaps unsurprisingly), the court rejected that argument and awarded the FTC summary judgment. (Read more at [www.ftc.gov/system/files/documents/cases/141018universalorder.pdf](http://www.ftc.gov/system/files/documents/cases/141018universalorder.pdf).) That's where the case seemed to take a disturbing turn. When asked to fashion a remedy, the court—while never finding that UPS was part of a “common enterprise” with the telemarketing defendants—held that UPS was responsible for the entire consumer harm caused by the telemarketers under Section 13(b) of the FTC Act. That is, while the fraudulent telemarketers themselves settled for virtually nothing, UPS, which had netted just a few thousand dollars in processing fees (before giving more than \$400,000 in refunds to injured consumers pre-judgment), was held jointly and severally liable for \$1.7 million—the totality of the telemarketers' processing activity minus only chargebacks and refunds. (Review the judgment here: [www.ftc.gov/system/files/documents/cases/150520universalmanagementjudgment.pdf](http://www.ftc.gov/system/files/documents/cases/150520universalmanagementjudgment.pdf).) Such a result, if left intact, had the

potential to have an incredibly chilling effect on processors' willingness to work with other high-risk, even if wholly legitimate, businesses. After all, the amount of the judgment against UPS was orders of magnitude greater than the fees it received from the parties' processing relationship. But it was not just an unsettling award from a proportionality perspective. As UPS argued on appeal to the Eleventh Circuit, the award did not seem sustainable under Section 13(b) of the FTC Act, which contemplates a defendant's “disgorgement” of ill-gotten gains, not the gains received by third parties (such as the deceptive telemarketers themselves). As UPS persuasively argued before the appellate court, the concept of a “joint-and-several equitable disgorgement” had little to no precedent outside of the context where the party assisting and facilitating the fraudulent conduct was part of a “common enterprise” with the other bad actors.

While not expressly holding that the district court “got it wrong,” the Eleventh Circuit seemed notably troubled with the result. It questioned how the district court had arrived at such a severe sanction and, forecasting its disinclination to affirm such an outcome outside

the context of a “common enterprise” or other uniquely extenuating circumstances, explained:

*If UPS was not included in the common enterprise, then the district court provided no explanation as to why joint and several liability in the amount of \$1,734,972 was appropriate, and made no findings which made such an award obviously appropriate. Accordingly, we vacate the judgment of the district court with respect to UPS...and remand this case for findings of fact and conclusions of law as to whether and why UPS is jointly and severally liable for restitution and in what amount.*

(Read the court's full opinion here: [media.ca11.uscourts.gov/opinions/unpub/files/201511500.pdf](http://media.ca11.uscourts.gov/opinions/unpub/files/201511500.pdf).)

On its face, the import (and importance) of the Eleventh Circuit's reasoning is difficult to ignore. For the first time, and at the highest level to date, there is judicial pushback against the idea that a processor or an ISO should be held liable for the entirety of the harm caused by its merchants' misdeeds. Rather, the Eleventh Circuit seemed to suggest that where a processor or ISO is not determined to be part



February 14-16, 2017 Berlin



MPE introduces

## „Festival of European online payment methods“

THE only European forum for merchants, online payment methods and payment providers



1000+ ATTENDEES



300+ C-LEVEL EXECs



150+ SPEAKERS



70+ SPONSORS & EXHIBITORS



300+ FINTECH PEERS



40+ COUNTRIES

[www.merchantpaymentsecosystem.com](http://www.merchantpaymentsecosystem.com)

of a “common enterprise” with a deceptive merchant, an equitable remedy should be crafted based on what the processor or ISO received from the processing relationship—not the totality of the merchant’s transactions. In short, the appellate court’s reasoning offers a glimmer of hope that the arc of Operation Choke Point may be headed toward a more positive, and proportional, direction.

That said (and somewhat surprisingly), the district court, on remand, seemed unmoved by the Eleventh Circuit’s suggestion that joint and several liability should attach only in cases where a “common enterprise” existed between the merchant and the processor or ISO defendant. In a decision issued in late October 2016, it instead re-entered its original award, reasoning that in other FTC cases (and in cases brought by the SEC), courts had imposed joint and several liability in certain circumstances, providing precedential support for its earlier decision. The court stopped short, however, of issuing any factual findings supporting the existence of a common enterprise. In doing so, it left largely unaddressed the Eleventh Circuit’s articulated concern that the original award lacked the factual predicates necessary to

sustain joint and several liability. Consequently, another appeal, and another opportunity for a federal court of appeals to address the appropriate contours of liability under the FTC Act, seems highly probable.

Of course, even if the Eleventh Circuit were to once again reverse the lower court, it would hardly defang Operation Choke Point. First, the Eleventh Circuit was focused on Section 13(b) of the FTC Act, which permits only equitable relief (and, interestingly, was the sole statutory authority invoked by the FTC in briefing related to the appropriate remedy). The court did not explicitly address Section 19 of the Act, which authorizes “such relief as the court finds necessary to redress injury to consumers or other persons” in instances where a defendant violates a *specific* rule, such as the TSR. Thus, while it may be cause for optimism in cases where the FTC is pursuing a processor or ISO for generic “unfair” or “deceptive” conduct, the Eleventh Circuit’s decision may not offer the same degree of comfort in other cases brought under the TSR. Second, even if the courts were to find disgorgement to be limited to the ill-gotten gains of a *particular* defendant, the standard for disgorgement in

FTC litigation remains a painful one. Under prevailing precedent, such disgorgement is calculated as the defendant’s *gross* receipts, which do not take into account expenses, including, for example, hefty residuals to sub-ISOs or sales agents. (For more, see *FTC v. Washington Data Resources Inc.*, 704 F.3d 1323, 1326–27 (11th Cir. 2013): [www.ftc.gov/system/files/documents/cases/universalsmithorder.pdf](http://www.ftc.gov/system/files/documents/cases/universalsmithorder.pdf).) Thus, a processor or ISO called upon to make disgorgement has the potential to lose much more than it ever netted in its relationship with a dubious merchant.

Even a more proportional Operation Choke Point has significant teeth and counsels strongly in favor of rigorous underwriting and risk-monitoring standards designed to prevent and detect consumer fraud. **TT**

---

*Edward A. Marshall is a partner at Arnall Golden Gregory LLP, in Atlanta, Georgia, where he co-chairs the firm’s payment systems team. He also serves as a member of the ETA’s Risk, Fraud, and Security Committee and co-chairs the payment systems litigation subcommittee of the American Bar Association Section of Litigation.*

## ADVERTISERS INDEX

Company	Page	Phone	Web
Apriva	11	877/277-0728	<a href="http://www.apriva.com">www.apriva.com</a>
Authorize.Net	C3	425/586-6000	<a href="http://www.authorize.net">www.authorize.net</a>
eProcessing Network, LLC	19	800/296-4810	<a href="http://www.eprocessingnetwork.com">www.eprocessingnetwork.com</a>
EVO Payments International	1	800/227-3794	<a href="http://www.evopayments.com">www.evopayments.com</a>
iPayment	5	617/681-6422	<a href="http://www.ipayment.com">www.ipayment.com</a>
Magtek, Inc.	C4	562/546-6603	<a href="http://www.magtek.com">www.magtek.com</a>
Merchant Choice Payment Solutions	C2	281/583-4400	<a href="http://www.mcpscorp.com">www.mcpscorp.com</a>
Merchant Payments Ecosystem	26		<a href="http://www.merchantpaymentsecosystem.com">www.merchantpaymentsecosystem.com</a>
USA ePay	24	866/812-3729	<a href="http://www.usaepay.com">www.usaepay.com</a>

# Kurt Strawhecker



Already a seasoned ad executive, Kurt Strawhecker joined First Data in the 1980s and started a marketing division that reportedly put the first stuffers in credit card statement envelopes. Then, a decade ago, he and Jamie Savant launched the Strawhecker Group, which the founders say mixes lengthy experience with Big Data to advise clients on all aspects of payments. Here, he leverages both to offer some insights on the industry.

### You grew up in Omaha. Is that why you based your consulting firm there?

Omaha is a payments-focused place, probably second only to Atlanta in terms of the payments-related jobs in the city. We've calculated there are somewhere between 10,000 and 12,000 payments jobs in Omaha, spread among PayPal, First Data, TSYS, and ACI Worldwide. There's a large number of spinoffs of those companies that's created other tangential payment companies.

### Can you use data to predict merchant attrition?

We collect merchant-level data—not transaction-level data—refreshed on a monthly basis by members of the database. The merchants are giving us 60 or more data elements. We determine what is occurring and what has occurred in order to predict the future. Payments companies use the information in all elements of their companies, like financial, sales, and strategy. And the data answers questions. “What should my pricing be for a million-dollar merchant in Savannah, Georgia?” “What verticals are underserved and offer greater opportunity?”

### What other trends does your data indicate?

A myth you hear is that our industry is in a race to zero, but profitability among merchants has been maintained. Meanwhile, the use of electronic payments is expanding at existing merchants as consumer habits change, and different types of merchants are now able to utilize electronic payments. Now you can pay with

plastic for a salad at McDonald's. Five years ago you couldn't.

### How else is the industry changing?

It's clearly becoming more complex because there are so many different players. Where 10 or 15 years ago you had very distinct roles—a third-party processor versus a financial institution, versus the brands, versus acquirers—the lines have now blurred. You've got the networks owning gateways. You've got third-party processors owning merchants. Gateways are being run by processors.

### Is specialization on the rise?

There is a higher degree of specialization. Being an acquirer that services all types of merchants is becoming more difficult with the proliferation of software vendors that are selling their software to run a merchant's business. The ISVs meet the very special needs of a particular type of merchant, and payments have had to change to interact with those software vendors.

Rather than going away, ISOs are becoming specialized to penetrate individual verticals. That can be everything from specializing in technology to specializing in sales technique to specializing in know-how—really understanding a particular type of industry vertical. Specialization from all sides.

We marvel at the way acquirers continue to evolve to match what the market is demanding. In this business if you don't, you lose. It's always been a changing industry. People in this industry are used to trying to be ahead of the game, trying to predict what will be most effective as

the industry continues to change.

The other great element of this industry is it has grown at a 10 percent clip for the last 10 years. The whole ocean is rising, as opposed to a zero sum game. That has helped foundational players as well as new technology players.

### What about consolidation?

We sat down and looked at our data. It surprised us that there's actually less concentration of volume in the top 10 acquirers today than there was 20 years ago. Think of the headlines of the last couple of years: Global buys Heartland, Vantiv buys Mercury. For every one of those acquisitions, we see 10 more ISOs starting up and specializing in individual sectors. Square didn't exist 10 years ago, and they're now in the top 30 merchant acquirers. With special pricing and a dongle, Square approached a certain size merchant very effectively.

### What's up with EMV—what has delayed it?

EMV took the industry by surprise even though it shouldn't have. We all knew EMV was coming, but most of the industry truly believed it would be delayed another year. Second, it's not boasting to say it's more complex here—not because we're smarter or faster, but because of a greater proliferation of types of payments companies. Third, there are so many devices and so much software to certify. **TT**

—Ed McKinley

# Celebrating 20 Years of Partnership



Since 1996 we have helped our resellers grow their portfolios. Working together with partners.

**That's what we do.**



**Authorize.Net®**



## eDynamo

### Secure Mag/EMV Chip Reader

Accept both EMV chip cards and magstripe cards with the eDynamo mobile secure card reader authenticator. Connect wirelessly to iOS and Android devices or connect to Windows PCs with a USB cable.

The eDynamo leverages the MagneSafe Security Architecture, including advanced encryption and card authentication, so you can process highly secure transactions with confidence. And the low energy consumption means the battery lasts even longer between charges, keeping you up and running while you're on the go.



**FIND OUT  
MORE** ▶

☎ 562.546.6467  
✉ [sales@magtek.com](mailto:sales@magtek.com)  
📍 [www.magtek.com](http://www.magtek.com)

EMV



Magstripe



Bluetooth



USB

