Exclusive: Fifth Annual Payments Technology Buyers' Guide PAGE 22

September/October 2015

TRANSACTION *trends*

ETA
THE OFFICIAL PUBLICATION OF THE
ELECTRONIC TRANSACTIONS ASSOCIATION

EMV 2.0

Where We Are
and What To Expect
After **October 1**

ALSO INSIDE:

THREE DECADES OF INNOVATION
ENSURING OUR PARTNERS' SUCCESS

PS

Positively Outstanding Solutions

TM-T88V | TM-H6000IV | TM-U220 | OmniLink® i | TM-m30 | TM-m10 | Mobilink™ P80 Plus

NEW MOBILE POS

For over 30 years, Epson has been a leader in the POS industry. Our POS printers are at the heart of thriving retail and hospitality businesses around the world. With the broadest product line available, Epson has set the standard with solutions that deliver unmatched reliability, speed and flexibility. And we're continuing to lead the way forward with our innovative, new tablet POS solutions, all designed with one goal in mind: your success. To see our latest solutions, **visit epson.com/pos**

EPSON®
EXCEED YOUR VISION

EVO® PAYMENTS INTERNATIONAL

NON-CASH PAYMENT SOLUTIONS AVAILABLE ANYTIME, ANYWHERE

As a leader in the payments industry, our mission is to forge partnerships through our innovative, reliable and secure payment solutions. We deliver value-added products and services and process over 50 billion dollars in transaction volume annually. These customized solutions reach more than 400,000 merchant businesses, in a variety of industries and sizes worldwide.

Our strong infrastructure and state-of-the-art payment platforms ensure safe and secure payment transactions, allowing us to provide the most advanced payment options needed in the market today.

- > Card Processing Services
- > Smart Mobile Payments
- > Fraud & Security Prevention
- > Risk Management
- > Accelerated Funding
- > Integrated Solutions
- > E-commerce Solutions
- > Cash Advancements
- > Online Payment Acceptance
- > Recurring Billing
- > Merchant Reporting
- > Gift and Loyalty

Smart partnerships build success.

Visit www.EVOpayments.com or call 1.800.227.3794
United States | Canada | Europe

PLANET Group Inc.

Acquire360

Complete Merchant Settlement, Accounting and Exception Management System

Challenge us for better interchange with Planet Group and Acquire360!

- Interchange Optimization
- Margin Improvement
- Better Profit Valuations

Contact us today to take control with Acquire360, and be your own processor!

Support for all major card types and multi-currency, including:

VISA MasterCard DISCOVER AMERICAN EXPRESS $ € £ ¥ ₩

PLANET Group Inc.

+1.800.979.9166

planetgroupinc.com
info@planetgroupinc.com

contents

The Official Publication of the Electronic Transactions Association Vol. 20 | No. 5

features

departments

Electronic Transactions Association
1101 16th Street NW, Suite 402
Washington, DC 20036
202/828.2635
www.electran.org

ETA CEO Jason Oxman

COO Pamela Furneaux

Director, Education and Professional Development Rori Ferensic

Director, Membership and Marketing Del Baker Robertson

Director, Communications Meghan Cieslak

SVP, Government Relations Scott Talbott

Director, Industry Affairs Amy Zirkle

Publishing office:
Content Communicators LLC
PO Box 223056
Chantilly, VA 20153
703/662.5828

Subscriptions: 202/677.7411

Editor
Josephine Rossi

Editorial/Production Associate
Christine Umbrell

Art Director Janelle Welch

Contributing Writers
Maayan Lattin, Edward A. Marshall, Ed McKinley, Julie Ritzer Ross, Josephine Rossi, and Scott Talbott

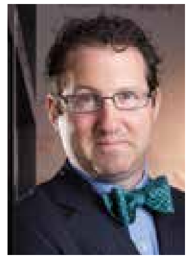
Advertising Sales
Alison Bashian
Advertising Sales Manager
Phone: 703/964-1240 ext. 28
Fax: 703/964-1246
abashian@conferencemanagers.com

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.**

@ETA

Shift Forward With ETA!

It's here—the date we've all been anticipating, the start of the U.S. shift to the Europay, MasterCard, and Visa (EMV) standard. Coordinating implementation among issuers, acquirers, processors, ISOs, equipment manufacturers, and the more than 8 million merchants in the United States is an enormous task. Fortunately, ETA is mobilized, deploying the resources you need to advance your business and educate merchants on the new EMV security standard.



While most large merchants have completed the work of upgrading, many small and medium businesses are still evaluating when to make the investment in their infrastructure. To help those merchants understand the benefits of upgrading to a more secure infrastructure, ETA is your source for original, essential, and unbiased EMV information. This year, we launched our merchant-facing website, SellSafeInfo.org, the leading source for information on payments security technology. Additionally, we have created and curated custom video-shorts, in-person and virtual peer meet-ups, ETA-exclusive webinars, and more, empowering our member companies and their customers to manage the EMV transition.

October's ETA Strategic Leadership Forum in Scottsdale, Arizona, will be the payments executive's window to the future of payments. Each year, this exclusive c-suite gathering provides actionable intelligence to the leaders who are accelerating the electronic payments universe.

And, to ensure that our member companies stay on the cutting edge of payments technology, ETA is returning to San Francisco to produce our newest event, TRANSACT Tech, on November 10. TRANSACT Tech will connect the most innovative companies in payments, technology, and global commerce to discuss the products and services they are deploying and the evolving point of sale.

Join me, and the Electronic Transactions Association, as we welcome EMV today, and prepare to meet future payments technologies tomorrow!

Jason Oxman
Chief Executive Officer
Electronic Transactions Association

25 ETA 1990-2015
ELECTRONIC TRANSACTIONS ASSOCIATION
Advancing Payments Technology

Millennials' Trust in Digital Security Low

U.S. and U.K. millennials could be losing faith in the digital economy, according to a new consumer survey commissioned by digital identity software firm Intercede and conducted by Atomik Research. Less than 5 percent of respondents believe their identity and personal data are "completely protected by effective safeguards."

The research questioned approximately 2,000 16- to 35-year-olds from the United Kingdom and the United States on their perceptions of current security measures. When asked about the effects of "an increasingly digitally connected world, such as the increased use of mobile devices and tablets on their digital privacy," roughly 70 percent said the risk will increase, with 31 percent saying the increase will be dramatic, according to a press release. More than half (54 percent) say the "failure of companies and governments to adequately protect identities and data would result in public distrust of goods and services." Forty-four percent say a decline in data sharing will result. "Smaller but still significant percentages of the research group said there is potential for a decline in economic or political stability," the release said.

Interestingly, the release also described a "millennial malaise" toward password-based authentication methods. Over the course of a year, one quarter of participants access more than 20 password-protected websites, applications, or devices. Forty-five percent only change passwords "when they have to," yet only 6 percent believe their data is "completely secure based on the password policy they apply."

Fast Fact

Financial institutions estimate the **cost of an EMV chip debit card will be double that of a standard magnetic-stripe card**. Large banks report the lowest average cost ($2.17 per chip card), while credit unions have the highest ($2.90 per chip card).

Source: PULSE, 2015 Debit Issuer Study

One Quarter of Brits Say They Won't Need Cash in Five Years

More than 40 percent of U.K. adult bank account holders say contactless payments are the future, while 25 percent think they will not need cash in five years, according to the latest online research from Lloyds Bank on the future of payments.

The majority of people surveyed believe they will still be using credit and debit cards (63 percent) and cash (52 percent) as daily methods of payments by 2025, while 48 percent expect to be using contactless payments daily. In addition, 27 percent expect to be making payments via wearable technology, 22 percent say they will be regularly using their fingerprint, and 7 percent believe they will make payments using a microchip embedded in their body by 2025.

Regarding mobile payments, 34 percent expect to be using a mobile device daily for payments in the next five years. Still, almost half say they "don't feel that mobile will ever be a main method of paying for goods and services," according to study results. Further, 44 percent say they don't use mobile devices to make payments because they don't think it is safe, followed by 18 percent who do not have the necessary phone; 17 percent who are unfamiliar with mobile payments; and 16 percent who "do not know how to use the technology."

Other results from the survey:

- Half of participants ages 55 to 75 are likely to think that they will always need to have cash, compared to 40 percent of respondents ages 18 to 54.
- Almost one in 10 (9 percent) of those over 45 think they will still be paying by check in 2025 compared to 4 percent of 18- to 44-year-olds.
- Women (46 percent) are more likely to think they will always need to have cash in the future compared to men (40 percent).

Breaches Up, Compromised Data Down in 2015

For the first six months of 2015, 888 data breaches occurred, compromising 246 million records worldwide, according to Gemalto's Breach Level Index. Compared to the first half of 2014, data breaches increased by 10 percent while the number of compromised data records declined by 41 percent during the first six months of this year. The firm attributes the decline in compromised records to fewer retail "mega breaches" this year.

The largest breach in the first half of 2015, which scored a 10 out of 10 for severity, was an identity theft attack on Anthem Insurance that exposed 78.8 million records. This event represented 32 percent of all data records stolen in the first six months of 2015, according to the findings report. Other notable breaches include the U.S. Office of Personnel Management (21 million records); a breach at Turkey's General Directorate of Population and Citizenship Affairs (50 million records); and a breach at Russia's Topface (20 million records). The top 10 breaches accounted for more than 81 percent of all compromised records.

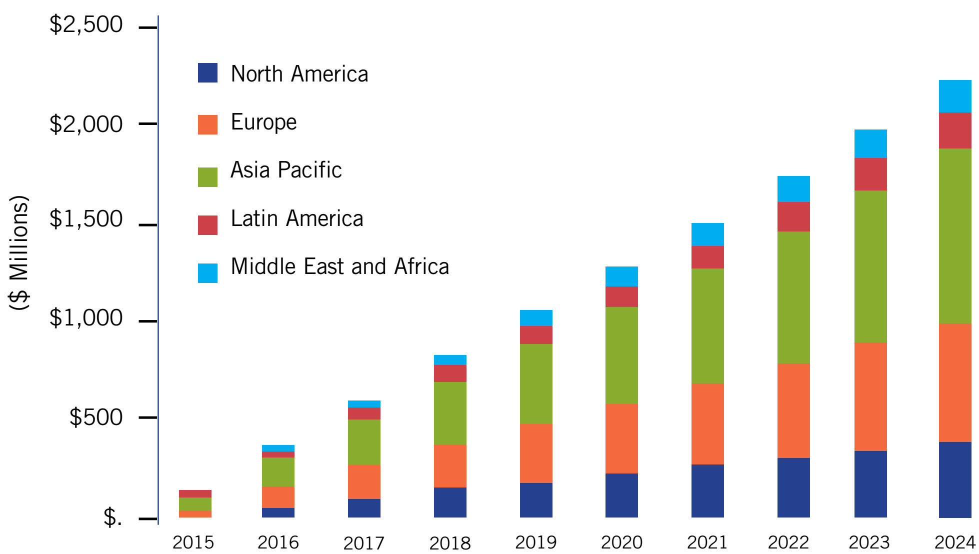
Two percent of data breach incidents were state sponsored, but the number of records compromised as a result totaled 41 percent of all records exposed. At the same time, "malicious outsiders were the leading source of data breaches in the first half of 2015," accounting for 546 breaches (62 percent), down 4 percent from last year. Forty-six percent, or 116 million, of the total compromised records were due to malicious outsiders, down 26 percent from 2014.

Other findings:

- Identity theft remained the primary type of breach, accounting for 75 percent of all records compromised and 53 percent of data breaches.
- The level of encryption used to protect exposed data increased slightly to 4 percent of all breaches, up 3 percent from 2014.
- Government and health-care sectors accounted for 31 percent and 34 percent, respectively, of compromised data records. However, breaches in health care accounted for 21 percent of breaches this year, down 8 percent from the same period last year.
- The number of stolen data records dropped significantly, accounting for 4 percent compared to 38 percent for the same period in 2014.
- The United States had the largest share of data breaches (76 percent) and nearly half of all compromised records (49 percent).

Infographic

Finance Biometrics Hardware and Software Revenue by Region, World Markets



Source: Tractica

PII Use Tops Trends in Online Fraud

Unlike previous e-commerce industry breaches, recent attacks are growing in size and targeting more valuable personally identifiable information (PII), says security technology provider NuData Security, which analyzes and scores billions of e-commerce shoppers and websites around the world.

The firm reviewed 5.1 billion "behaviors" from May through July 2015. Of the more than 500 million account creations analyzed, more than 57 percent were flagged as high risk or fraudulent, compared to 28 percent in February through April. Account creation fraud has increased by more than 100 percent since February 2015.

Other trends researchers observed include:

- Nearly half of all account registration fraud attempted in May was tied to creating false accounts to deliver false product ratings.
- Incidents were traced back to 151 countries, but a significant portion of attacks originated from China and the United States, followed by Saudi Arabia, the United Kingdom, Malaysia, and Brazil.

Data breach notification and reloadable prepaid cards among the topics receiving attention from lawmakers

Autumn in Washington

By Scott Talbott

With the last few months of the year upon us, Congress and the nation's regulators are focusing on myriad issues facing the payments industry. Let's take a look at what to expect from the activity in Washington, D.C., this fall.

Data Breaches and Cybersecurity

With the October 1 shift to the Europay, MasterCard, and Visa (EMV) standard, and the prevalence of data breaches throughout the country, consumer data protections are at the forefront of policymakers' minds.

One issue that is currently in the spotlight is consumer breach notification. Currently, when a data breach occurs, companies must follow a patchwork of 47 different state laws to notify their customers. The payments industry, along with retailers and others, continues to press Congress to create one uniform federal standard for breach notification. Five bills have been introduced to achieve this goal. ETA is strongly supportive of this initiative.

Another topic being debated is information-sharing about cyber threats. The payments profession is on the front lines on the war against cybercrimes. As an industry, we see the individual data points before they form a pattern of a cybercrime. Currently, a company with information about a potential cybercrime is prohibited from sharing it with the U.S. government, thereby weakening our defenses. ETA supports allowing companies and the government to voluntarily share information about cyber threats. Doing so will strengthen our industry's ability to monitor, detect, contain, and prevent cybercrimes. The House of Representatives has passed two bills on this issue, and a Senate bill is awaiting floor time.

We will all be watching to see what happens after October 1, which is the first day of the shift to EMV-chip cards. All of the players in the payments industry have been working hard to prepare for this day. Chip cards are being sent to customers, merchants are upgrading their POS terminals, and processors have adapted their systems. As the business side of the industry is preparing for the shift to EMV, lobbyists are hard at work in Washington, briefing policymakers on what the shift means to them and their constituents. ETA is providing regular briefings to Congress and federal regulators to offer education on chip cards. The briefings focus on the following:

- Type of fraud they prevent—counterfeit card fraud
- How the chip works—creating a special, one-time use code for each transaction

- What it means to consumers—no liability for fraud
- How chip cards fit in with other technology like tokenization and encryption.

The Congressional Payments Technology Caucus is holding its second briefing on September 24. The briefing allows industry experts to brief members of the caucus on the migration to chip cards. ETA members are part of the distinguished panel.

Regulatory Issues

As Congress grapples with legislation, federal regulators are thinking about how the new world of payments fits into the existing regulatory framework, and if any new regulations are needed.

One topic under discussion is the Consumer Financial Protection Bureau's (CFPB's) recently released 870-page proposal to regulate general reloadable prepaid cards. The proposal would create heavy regulatory burdens on mission-critical features of prepaid cards, including overdraft, and generate confusion among consumers regarding disclosure requirements. The proposal also attempts to regulate peer-to-peer lending, mobile transactions, and Bitcoin. The payments industry extolls the many virtues of prepaid cards, including ease of use, low fees, and an easy way to distribute payroll, student funds, and government benefits. The industry continues to express strong concerns with the restrictions proposed by the CFPB.

Another popular topic among regulators is Big Data, and its use by the business community. Big Data refers to the collection of lots of information about one person or a group of persons to enable the collector to mine the data for specific business purposes. The business community uses Big Data to target specific product offerings, to learn more about what consumers want, and to reduce fraud. Regulators are worried Big Data could be used for more nefarious purposes, like discrimination. Given the newness of the concept, the payments industry is urging regulators to go slow and not rush to regulate.

As far as state regulatory issues are concerned, ETA is working on a number of initiatives, including the attempt in Washington State to tax processors on interchange as it moves through the system.

Current ETA Government Affairs

The month of September is a busy one for ETA, with the following activities:

- **September 16: Policy Day.** ETA hosted the Technology of Fraud Prevention Policy Day with PCI in Washington, D.C. The event featured three panels of industry experts focused on chip cards, tokenization, and encryption. The audience comprised Hill staff, regulators, law firms, and other payments experts. ETA regularly hosts Policy Days to educate policymakers about the role of the payments industry in our economy.
- **September 17: Executive Fly-In.** More than 50 ETA executives traveled to Washington, D.C., to participate in more than 30 meetings with representatives from Congress, CFPB, the U.S. Department of the Treasury, and the Federal Reserve to talk about the EMV shift and legislation to protect consumers from cybercrimes.
- **September 29: Webinar on Policy Threats From Washington, D.C.** ETA hosted a policy-focused webinar that covers how lawmakers and federal regulators are focusing on the payments industry; with the stroke of a pen, policymakers can change the way payments professionals do business, as well as their bottom line. The webinar featured an in-depth look at the threats from Washington, such as Operation Choke Point, as well as what ETA is doing to represent your interests, and how you can get involved to help promote good public policy and defeat bad policy ideas.

There are only a few more work weeks left for Congress in 2015, and it is important for industry executives to have their voice heard to ensure that premature or overreaching regulators do not interfere with the industry's efforts to innovate and deliver better products and services to consumers. ***TT***

Scott Talbott is senior vice president of government affairs for ETA. For more information, contact Grant Carlson, government affairs coordinator, at 202/828.2635.

IT'S OCTOBER 1— Now What?

Experts weigh in on the EMV deadline and what to expect in the months ahead

By Ed McKinley

Earn ETA CPP Continuing Education Credits
Throughout 2015, *Transaction Trends* will provide readers with executive summaries of ETA whitepapers and industry thought leadership. Read this article, then visit http://www.electran.org/eta-cpp-quiz-emv to test your knowledge and earn 2 ETA CPP CE credits per quiz!

ETA ELECTRONIC TRANSACTIONS ASSOCIATION

The much-anticipated Europay, MasterCard, and Visa (EMV) liability shift has arrived—but October 1 is just another day of small victories in the long, hard slog toward converting a nation to chip cards.

"The date will come and go, and some of us will feel that not much has happened," says Michael Moeser, an analyst at Javelin Strategy & Research. "The reality is that it's going to take time."

At issue is the switch from payment cards that carry a small amount of data in a magnetic stripe to cards embedded with a tiny computer chip that holds much more information and offers much greater security. Although the card brands decreed that liability for card fraud that EMV could have prevented shifts to merchants as of Oct. 1, 2015, only about half of small retailers and restaurant proprietors were expected to be ready to accept EMV cards on that day, Moeser says.

Generally, the mammoth retailing chains outpaced smaller merchants in the quest to accept EMV cards, according to J. Craig Shearman, vice president of government affairs public relations for the National Retail Federation (NRF), an industry trade group. A survey of the NRF's CIO Council, which comprises chief information officers at mostly large but a few medium-sized retailers, indicated 90 percent would be ready for EMV by the date of the shift or at least on their way to readiness, he says.

Walmart, which *Fortune* magazine ranks as the world's largest company by revenue, had the resources to beat the deadline, published reports say. Target, the retailing giant that suffered an infamous data breach in late 2013, brought its power and influence to bear on the transition and will still barely make the deadline, according to those reports.

Although those chains prepared themselves for EMV by the appointed date, their efforts may seem tardy from a global point of view. That's because the United States was the last major economy to switch to chip cards. The nation's reliable and relatively inexpensive phone service does a good job of carrying mag-stripe data. That wasn't the case elsewhere in the world, and most of the planet shifted to EMV early on, making their transactions safer and causing criminals to turn their attention to less-secure American mag-stripe transactions. As a result, as card-present fraud decreased in other countries because of EMV, it increased in the U.S. because of the lack of EMV. *(Editor's Note: Because EMV makes a major impact on lost/stolen fraud, criminals will move to other types, particularly card-not-present fraud, according to data from other countries. Read "Lessons Learned" in our January/February 2015 issue for an in-depth analysis of the relationship between EMV implementation and fraud on a global scale: http://bit.ly/1Use2Uo.)*

Still, card fraud doesn't necessarily frighten America's small and medium merchants. For some, it's a case of blissful ignorance, says Moeser. An August Javelin study, called "Small Business EMV Readiness," indicated just 56 percent of retailers with annual sales of $10 million or less claimed they knew much about EMV or the PCI Data Security Standard.

Many merchants don't believe they need to become well versed in the standard and what it can do. Instead, they rely on their acquirers to provide them with the right state-of-the-art payments terminals and POS systems, says Donna Embry, senior vice president of Payment Alliance International, a merchant services provider and ATM deployer.

For a lot of the smaller merchants that have examined the situation, EMV doesn't bring an adequate return on investment, observes Mark Dunn, president of Field Guide Enterprises, a consulting firm for ISOs. If a merchant has an average ticket of $64 and upgrading to EMV costs $360, it makes economic sense to stick with mag-stripe readers.

"It's not a desperate situation for most merchants," Dunn says. "They should take their time, understand the issues, look at the alternatives, shop around a little bit, and then make their choice."

Leisure aside, however, there's the need to train sales associates to accept chip cards and familiarize the clientele with the new way of paying. Both of those prospects can seem unappealing to merchants narrowly focused on their core business.

"You could look at Oct. 1, 2020, and you're not going to have 100 percent of merchants that are EMV-capable," says Embry. "It's costly."

Conversations and Distractions

Meanwhile, EMV hasn't become the top priority for ISOs and acquirers, either, according to Rick Oglesby, a partner and head of product consulting and market research at Double Diamond Payments Research. While EMV provides an opening for conversations with merchants, acquirers are more interested in convincing customers to use Cloud-based mobile POS systems that provide multiple functions, such as inventory control and ordering. Acquirers can control those devices and use them to differentiate themselves and create lasting relationships with their customers, he says.

"IT'S NOT A DESPERATE SITUATION FOR MOST MERCHANTS. THEY SHOULD TAKE THEIR TIME, UNDERSTAND THE ISSUES, LOOK AT THE ALTERNATIVES, SHOP AROUND A LITTLE BIT, AND THEN MAKE THEIR CHOICE."

– MARK DUNN, FIELD GUIDE ENTERPRISES

Of 26 payment-processing companies that participated in Double Diamond's "To Be or Not to Be an ISV? Integrated Payments Strategies for Merchant Solutions Providers" survey conducted early this year, 30 percent of ISOs and acquirers were interested in working with a vendor to help promote EMV, Oglesby says. Meanwhile, 72 percent wanted a vendor's help with mobile POS; 68 percent were seeking a vendor for digital loyalty; 62 percent wanted a vendor for semi-integrated payments solutions; 58 percent were seeking one for integrated payments; and 46 percent wanted one for an e-commerce gateway, he reports.

That lukewarm overall support for EMV could slow the transition to the standard because many in the industry have assumed that ISOs and acquirers would take the lead in promoting chip card readers to small merchants. They're the logical segment of the industry to become EMV ambassadors because of their face-to-face relationships with merchants, industry observers agree.

Larger ISOs have formulated an effective EMV strategy that uses the standard to promote other services, such as security precautions, mPOS systems, and integrated software that helps them run their businesses, according to Dunn. Smaller ISOs and sales agents have lagged behind and have only a tentative grasp of EMV. Some of the smaller players will still be grappling with how to approach the subject when the liability shift occurs, he says.

But even when merchants and acquirers work diligently to meet the EMV deadline, their efforts are sometimes stymied by the huge task of getting all the necessary hardware and software to work together, Embry says. Terminal manufacturers have been cranking out EMV-ready machines since before the 2011 EMV announcement, but much work remains unfinished when it comes to testing and certifying that terminals, gateways, and processing platforms all interface properly in EMV transactions.

"It's very hard for a merchant to buy a truly EMV-ready solution," Oglesby agreed five weeks before the deadline. "Certification is significantly arduous. Every time you change a device or you change a line of code, it needs to be recertified." Connecting an EMV reader to a tablet, for example, would require certification. Changing a line of code would necessitate recertification. Oglesby notes that not many certification announcements were appearing as the deadline loomed.

"There have not been enough service providers or personnel provided to get the certification work done on time," Shearman asserts.

Others agree on the difficulties of certification. Dunn explains that roughly one month before the shift he worked with an ISO client that had an application in place for several years. "They [were] having great difficulty getting an affirmative response from the processor, saying that an upgraded device with upgraded EMV software [was] going to be available" by October 1.

That sort of situation prompts some ISOs and acquirers to sell EMV-ready systems with the promise to throw a switch in the Cloud when certification comes, Oglesby says, adding that there's not much more a merchant can do to comply.

Education

While the certification process continues, card issuers are working to put chip cards into the hands of consumers and teach the public how to use them. By the end of this year, issuers will have dispersed 166 million EMV credit cards and 105 million EMV debit and prepaid cards, which is 29 percent of all credit cards and 17 percent of all debit and prepaid cards, according to an April 2014 Javelin report called "EMV in USA: Assessment of Merchant and Card Issuer Readiness," Moeser says. By the end of 2018, EMV will reach 96 percent penetration of credit cards and 98 percent of debit and prepaid cards, he says.

The public is adapting to "dipping" EMV cards instead of "swiping" mag-stripe cards, Shearman says. Still, a few consumers forget to retrieve their cards after leaving them in the machine for the duration of the transaction instead of keeping them in hand during the swipe.

No one mounted a coordinated effort to teach the public how to use chip cards or why they're important, Dunn says. "The word isn't getting out," he maintained in a conversation just before the liability shift. "I'm disappointed that we're not seeing public service messages on television."

One reason for the "loose" approach to EMV in the United States was the card brands' collective decision to allow the free market to guide the transition, sources say. In other countries, central banks or government dictates led the switch to EMV. In the United Kingdom, widespread public relations campaigns accompanied the introduction of the standard.

Making the government a partner in America's transition would not have pleased some members of the payments industry here. Embry says the government would have added unneeded complexity, and she cites the Durbin amendment to the Dodd-Frank Act as an example. The amendment's stipulation that retailers must have their choice of at least two debit networks delayed the U.S. EMV transition, sources say, as the networks worked out how they would use technology to give merchants that choice.

"Other markets had four years for the migration, and the U.S.—the biggest and most complex market—had 18 months," Oglesby says of the delay that debit routing caused. "Some of the networks were considering extending the deadlines until we had the major breaches at Target and pretty much everybody on the major merchant list."

Whatever the timing, some groups took exception to the U.S. approach to EMV. The NRF complained about the country choosing chip-and-signature instead of chip-and-PIN for transactions because PINs offer more security, says Shearman. Proponents of signature say it's more familiar to consumers.

Groups such as the American Bankers Association say no one technology is "fail-proof." As part of its Let's Innovate, Not Mandate media campaign, the ABA cites a 2012 Federal Reserve Bank of Atlanta that found PIN debit fraud rates have increased more than threefold since 2004. It also says mandates hurt consumers because they direct resources toward technology that quickly becomes obsolete.

"If we mandated cell phone technology, we'd still have brick style phones," the ABA said in an advertisement appearing on Politico.com. "If Congress mandates a static payments technology, security safeguards will be out-of-date tomorrow."

A shift to near field communication should have accompanied the transition to EMV, says Embry. As it stands, "that could be a another round of changes, and it could have been accomplished in one fell swoop."

Offering a discounted interchange incentive would have hastened the transition, too, she says. EMV does nothing to make transactions easier for consumers or merchants, she notes.

Next Year

Whatever one thinks of the details, the next big event in the American transition to EMV is expected to occur early in 2016. That's when merchants will begin seeing enough chargebacks accumulating to cause alarm, Oglesby says. "It will be 90 days post deadline," he says. "That's when merchants will start to feel the pain."

The uptick in chargebacks will occur first in Miami, Chicago, New York, and other major cities—not in rural Iowa, Embry says. It might take eight months or a year before Des Moines gets hit as fraud spreads from the metropolitan centers, she predicts.

"SOME OF THE NETWORKS WERE CONSIDERING EXTENDING THE DEADLINES UNTIL WE HAD THE MAJOR BREACHES AT TARGET AND PRETTY MUCH EVERYBODY ON THE MAJOR MERCHANT LIST."

—RICK OGLESBY, DOUBLE DIAMOND PAYMENTS RESEARCH

"Roll the dice," Embry suggests. "If you think you're not going to get hit with a chargeback, then don't pay the money to upgrade your machine."

In the meantime, EMV will continue to distract the payments industry, Embry laments. "It keeps innovation at bay," she says. "The processors are so tied up with it."

Some have compared the EMV liability shift to Y2K, the threatened but unrealized breakdown of the world's computers at the beginning of the new millennium. But the comparison doesn't hold up for Dunn because the EMV transition is actually occurring. "EMV is real—it's just rolling slowly," he says. "The question is not whether you upgrade to EMV. It's when and how." ***TT***

Ed McKinley is a contributing writer to Transaction Trends. *Reach him at edmckinley773@yahoo.com.*

CLOs: Not Quite Ready for the Big Leagues

By Julie Ritzer Ross

While more marketers are adding card-linked programs to their lineup, better data analyses, connectivity with mobile wallets, and industry standards are needed

Over the past few years, card-linked offers (CLOs)—cash-back and discount deals tied to credit, debit, and/or loyalty card transactions—have become a viable loyalty marketing method and an alternative to traditional advertising and purchasing incentives. CLOs allow merchants the chance to engage more closely with customers, effectively cultivate repeat business, and possibly lure consumers away from the competition. For processors, handling these transactions is another revenue-generating service to promote to merchants. And as trusted advisors to merchants, ISOs can position CLO programs to sharpen their competitive edge and bolster profits.

Financial institutions such as Bank of America, whose BankAmeriDeals program runs on a platform developed by Cardlytics, and American Express, which leverages its proprietary processing network to run its AMEX Offers, have jumped on the CLO bandwagon. So have Foursquare, Microsoft, First Data, and Groupon, which are promoting CLOs to merchant customers and/or consumers.

Bonus Audio Content: Log in to listen to "Real-Time Card-Linked Loyalty and Promotions" from TRANSACT 15. Visit http://bit.ly/1y0ijag.

Still, despite being called "great promise" by one industry consultant, CLO programs have far to go to create long-term sustainability in the payments ecosystem. Even Bank of America, which claims to have provided targeted CLOs generating more than $730 million in measurable, incremental revenue for more than 4,000 merchants since 2012, must concede this. Bank spokespersons declined further comment, but the financial institution's statistics are telling. Specifically, 78 percent of chief marketing officers who participated in a Bank of America study conducted with marketing organization The CMO Club said they know what card-linked marketing is, but more than half (62 percent) had never implemented a program.

Although the bank's survey was conducted in 2014, "under-utilization is still the watchword when it comes to CLOs, and we continue to see only a small percentage of merchants implement them," asserts Peter Krasilovsky, vice president and chief analyst at BIA/Kelsey, a research and consulting firm specializing in media and marketing.

Nonetheless, more merchants are stepping up to bat, say Krasilovsky and other sources. Findings of a survey released in April by the CardLinx Association—a CLO industry group whose members include merchants, digital publishers, payment networks, and banks—show growth. Ninety-five percent of the 50 "largest companies in the [CLO] space" cited an increase in the number of merchants that had used CLOs within the previous 12 months, and more than 92 percent reported an uptick in the number of consumers who had done so during the same interval. Nearly one third of respondents pointed to annual CLO growth of more than 30 percent.

The study's results "demonstrate the accelerating momentum in card-linking, and the real value it delivers to consumers and merchants," Silvio Tavares, CardLinx Association president and CEO, said in a statement when the findings were announced. "Major advancements over the past year and heightened expectations among consumers and merchants have drastically increased card-linking's value proposition of better targeting, measurable ad spend ROI, and a seamless customer experience."

While not entirely quantitative, conclusions from the BIA/Kelsey "Status and Review of Card-Linked Offers 2015" survey of 14 "CLO industry leaders," including Vantiv and Heartland Payments, also make a case for CLO progress. "We learned during these calls that more merchants were utilizing CLOs at the end of 2014 than at the end of 2013," says Krasilovsky. Additionally, merchants appear to be earmarking more money for CLO. Budgets for initial endeavors typically ranged from $25,000 to $100,000, but new CLO commitments have more frequently entailed "seven-figure" contracts, he says.

The companies in the survey also are feeling "a certain degree" of consumer CLO momentum, Krasilovsky continues. Consumers not only are redeeming a higher number of CLOs, some respondents said, but they also are embracing CLOs with increased frequency. Only one company reported that its CLO response rate had remained the same for the six-month period preceding the study.

Positive Signs

If consumer attitudes and the perspectives of CLO-offering businesses are any indication, merchant adoption and cardholder use should steadily grow. For example, of the Bank of America survey participants who leveraged CLOs, nine out of 10 claimed the program lifted revenues for their companies. Ninety percent deemed CLOs an effective solution for reaching their target audience, and 96 percent said their companies plan to incorporate CLOs into future marketing campaigns.

"MAJOR ADVANCEMENTS OVER THE PAST YEAR AND HEIGHTENED EXPECTATIONS AMONG CONSUMERS AND MERCHANTS HAVE DRASTICALLY INCREASED CARD-LINKING'S VALUE PROPOSITION OF BETTER TARGETING, MEASURABLE AD SPEND ROI, AND A SEAMLESS CUSTOMER EXPERIENCE."

—SILVIO TAVARES, CARDLINX ASSOCIATION

"High CLO buy and conversion rates that fall above other promotional media are playing a role here," Krasilovsky points out. Respondents to the BIA/Kelsey survey reported per-customer unit CLO sales rates in the single digits monthly, with one respondent claiming that its customers routinely use CLOs to buy more than eight items every month, on average. Two respondents characterized their conversion rates at 3 to 12 percent.

On the consumer side, half are taking advantage of or are interested in trying CLOs, according to a March study conducted by Forrester Consulting, a unit of Forrester Research, for digital marketing platform provider Linkable Networks. Of these consumers, 55 percent would be "very likely" or "somewhat likely" to link their existing loyalty cards (such as grocery or pharmacy cards) to their credit or debit cards to participate in CLO programs. Fifty percent would be "very likely" or "somewhat likely" to link promotional offers and/or coupons to their credit cards.

Similarly, according to Cardlytics' 2015 "Card-Linked Marketing Consumer Sentiment Study" (completed with the Harris Poll), nearly two thirds (64 percent) of Americans believe CLOs would be helpful, with more than half (51 percent) saying it would help stretch money further. Roughly one third said they would have new shopping choices (32 percent), be able shop their favorite brands/retailers more frequently (31 percent), and be able to make purchases for which they have been saving (31 percent). The study also brings to bear a perception that CLOs are appropriate for and applicable in myriad scenarios. Eighty-three percent—of whom all are online or mobile banking users—stated that they would redeem CLOs during holidays and special events.

These findings "and the attitudes they represent are not really a surprise considering how much more attractive than straight points-based loyalty programs CLOs can be," observes Edward Niestat, managing director of the information management services practice at consulting firm AlixPartners. Points-based loyalty programs may yield bigger rewards, such as free merchandise, accommodations, and flights, but accruing the necessary points often requires time. By contrast, although programs like BankAmeriDeals provide cash back for purchases (deposited into cardholders' checking accounts) only once each month, it's quicker than waiting to accrue enough points for a sizeable reward, Niestat explains.

Rookies and Game Changers

Despite recognition of CLOs' potential, certain barriers to progress exist, and payments professionals can chalk at least part of it up to merchant ignorance.

"Whether it is because whichever (entities) are promoting CLOs are not doing the best job of explaining them, or they somehow cannot make a good business case for trying them out, there are players that just aren't looking seriously at the programs," says Richard Crone,

Millennials, Younger Parents Bullish on CLOs

Millennials ages 18 to 34 and parents of children under 18 living at home are more inclined to redeem card-linked offers (CLOs) than adults in general, according to a study conducted by Forrester Consulting, a unit of Forrester Research, for CLO platform provider Linkable Networks.

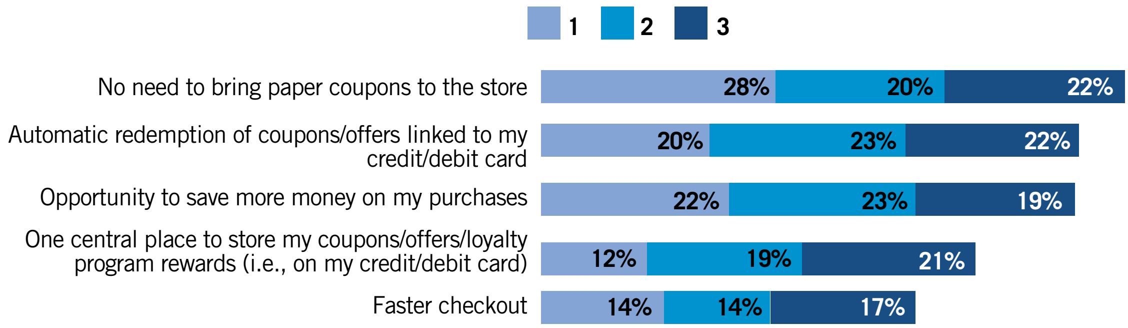
When asked how likely they would be to use card-linked offers instead of printing coupons from websites, 56 percent of adults in all age groups said they would be "somewhat" or "very likely" to do so. Sixty-five percent of millennials, and 62 percent of participants with children under 18, offered the same response. Similarly, 56 percent of all respondents, 58 percent of millennials, and 62 percent of parents whose youngsters are under the age of 18 said they would prefer to use CLOs instead of clipping paper coupons from newspapers and circulars.

The promise of CLOs may even be sufficient to induce some consumers to shift their allegiance from one merchant to another if the former did not have a CLO program but the latter did. Sixty-one percent of parents with children under 18 at home claimed they would do so, as would 48 percent of millennials and 40 percent of adults in general.

58 percent

of millennials said they would **prefer to use CLOs** instead of clipping paper coupons from newspapers and circulars.

What is most appealing to you about linking coupons and/or loyalty cards to your credit or debit card? Please rank your top three, with 1 being the most appealing.



Note: Based on 516 U.S. online adults

Source: A commissioned study conducted by Forrester Consulting on behalf of Linkable Networks, March 2015

CEO of payments consulting firm Crone Consulting LLC. Findings from the Bank of America survey support Crone's assertion: Of companies that have not used a CLO program, 53 percent blamed at least a portion of their reluctance on a lack of knowledge about how the programs work. One in three marketers expressed uncertainty about program effectiveness.

Statistics notwithstanding, certain changes must occur before the real marketing potential of card-linked programs is realized. Crone notes that the "game changer" will come not from linking offers to cards, but from "connecting" them to mobile wallets.

"There's no question that mobile payments and mobile wallets are going to become more and more popular, especially as mobile wallet alternatives to Apple Pay, like CurrentC and Samsung Pay," propel mobile wallet acceptance forward, he says. "The ability to receive and redeem CLOs within whatever mobile wallet they happen to carry will be a big deal for consumers; the more they can do this, the more [consumers] will take CLOs seriously."

In turn, Crone says, CLO platforms will need to feature open application programming interfaces (APIs) so that programs can be offered on traditional websites as well as easily integrated with mobile banking and retailer apps. Additionally, merchants and other entities that promote CLOs will need sophisticated data analysis engines to help deliver and redeem mobile CLOs in real time, rather than require consumers to ferret out options on their home computers and wait for redemption.

"For both mobile and nonmobile programs, another obstacle to adoption has been the fact that there's no immediate gratification—for example, consumers are forced to wait 30 days to receive cash back in their account or to see a reduction in the price of an item they bought using a CLO that promises a discount," Crone says. "All systems—mobile and otherwise—will need to be configured so that settlement occurs immediately at the point of sale."

This, the executive adds, is the "beauty" of CurrentC, which reportedly will offer net settlement on CLOs.

Moreover, the BIA/Kelsey survey demonstrates that the CLO experience for merchants also warrants improvement, Krasilovsky says. Although certain merchants are renewing and upgrading their initial CLO accounts, others have slowed down or put their programs on hold because the analytics are less granular than those from other marketing channels. For example, some want to vary their campaigns and entice new customers with higher discounts on purchases, but they feel they cannot do so without CLO-related analytics that allow them to distinguish new from existing customers. Others would like CLO platform providers to share larger volumes of data, and to assist in evaluating them.

Finally, industry standards for CLOs must be developed, say sources. In February, the CardLinx Association released the final versions of CLO standards intended to facilitate interoperability between CLO payments and digital marketing systems. The standards address common CLO advertising insertion orders, digital ad attribution performance measurement, fraud detection reporting, and the determination of which CLOs (and in what order) should be applied to a single transaction when a cardholder attempts to redeem multiple offers linked to one card. "This first set of voluntary standards represents a significant step forward in delivering scale and improving ease of use for merchants and consumers," which the association hopes will spark CLO adoption, says Tavares.

Krasilovsky agrees, but cautions that transformation will not occur overnight. "It's a journey," he says. "Card-linked programs will get there. It's like everything else. We need to be patient." ***TT***

Julie Ritzer Ross is a contributing writer for Transaction Trends. *Reach her at jritzerross@gmail.com.*

Discover® is Partnering with the POS Channel to Accelerate EMV Deployment

By John Badovinac
Head of Integrated Payments Discover Financial Services

Discover® is Engaged with the Channel on EMV

For the past several years Discover has been in discussions with key participants in the integrated Payments Channel in order to help plan for and accelerate EMV deployment. Discover has conducted EMV engagement discussions with the top ISVs in the channel in order to share information and validate EMV enablement plans. These ISVs account for the majority of merchants enabled within the POS ecosystem. These discussions have been beneficial to both parties as we have identified several ways to align interests and accelerate deployment of the Discover EMV specification called D -PAS. Discover recognizes that ISVs have a variety of solutions that they can explore to enable their merchant portfolios for EMV acceptance and this engagement has proven to be very valuable to our partners as they explore options including direct payments application integration, semi-integrated options, and solutions provided by Gateways and hardware providers.

Discover Offers Resources for EMV Deployment

After listening to channel input, Discover has developed an engagement plan and resources that our channel partners can put to work to assist them in developing and deploying their EMV solutions. The Discover engagement plan helps to ensure ISVs help Discover achieve our objectives

within the channel including: ensuring ISV applications enable the full set of Discover card ranges for transaction routing, engaging the ISV's Dealer network to educate them on Discover programs, and partnering to communicate Discover Acceptance at the cashier level. The greater the alignment of interests achieved with our ISV partners, the greater the resources Discover can make available to targeted partners. These resources include financial incentives for coding to support the Discover D-PAS EMV specification, access to third-party EMV certification tools to speed EMV card brand certification, and education support for rollout of the ISV's EMV solution to their Dealer base. Most recently we partnered with Shopkeep to promote and accelerate EMV

deployment. David Herzog, Director of Business Development at ShopKeep said, "Shopkeep is pleased to have the support and resources provided by Discover as we deliver our EMV capable solutions to our merchants."

Discover is committed to celebrating partner's EMV Success

The channel's response to the Discover EMV engagement plan has been exceptionally positive. We are currently in EMV deployment discussions with the majority of our ISV partners, their Acquiring partners, and supporting Gateways. We look forward to celebrating and supporting these early deployments throughout the year both in the press and by partnering with engaged clients with whom we can promote mutual goals at industry events. To learn more about the Discover D-PAS EMV enablement resources please contact your Discover Relationship Manager. We are excited to share information and resources that support our common goals with D-PAS EMV deployment.

TRANSACTION trends

Who's Who in Payments Technology

Our fifth annual directory unites payments professionals of all specialties to meet the diverse needs of merchants and their customers

Today's savvy consumers understand there are many ways to both shop and pay for products and services in a technology-driven society. As more consumers become comfortable with mobile wallets and payment apps, they will demand the opportunity to purchase goods using their method of choice. Merchants who hope to remain profitable long into the future must adapt to integrate electronic channels into their business operations. And that's where payments professionals come in.

Payments companies that offer products that make it both easy and secure for merchants to accept a wide array of payments are in great demand. While most consumers still carry some cash, they're using it less frequently and only for select purchases, such as street vendors and cabs, according to Walker Sands' "2015 Future of Retail Study." What's more, the introduction of Apple Pay, Samsung Pay, and various other competitors and partners has accelerated that shift.

As we move toward a more "cash-less" society, merchants and payments professionals have new opportunities. "It's clear that consumers are experimenting with mobile wallets and apps and are intrigued by the possibility of Apple Pay pushing smartphones into the mainstream," notes the Walker Sands study. "At the same time, consumers are hesitant to fully embrace mobile payments entirely because of security and privacy concerns. But with cash on the decline and hacking scandals eroding trust in traditional point-of-sale systems, retailers who embrace mobile payments and convince consumers it's a safe way to make a purchase might be able to offer the best of both worlds."

Moving to Mobile

The future of mobile payments is expanding, with more consumers using their mobile phones to comparison-shop and obtain product information while in retail stores. Of U.S. smartphone users who use apps, 18 percent accessed at least one mobile wallet app during the average month in the first quarter of 2015, according to Nielsen statistics. Those who are using mobile wallets are an attractive demographic for merchants: Twenty-nine percent

are ages 29 to 44, and 20 percent are ages 25 to 34, according to the Nielsen Company.

While there has been a significant increase in "showrooming"—the practice of visiting a store or stores to examine a product before buying it online at a lower price—the continued popularity of bricks-and-mortar stores should not be minimized. Thirty-nine percent of all mobile payment users with smartphones made a POS payment using their phone in the previous 12 months, according to "Consumers and Mobile Financial Services 2015," published by the Board of Governors of the Federal Reserve System.

"Total Retail: Retailers and the Age of Disruption," an annual survey of shoppers undertaken by PriceWaterhouse Coopers (PWC), also found that physical stores are still primary destinations for shoppers. Only 27 percent of U.S. consumers say they shop online weekly; 65 percent noted they prefer in-store shopping because they want to avoid delivery fees and want to have products immediately, according to PWC data. As a result, retail stores that make a number of payments options available stand to benefit from repeat business.

One area that both payments professionals and merchants need to watch is the growth of merchant-based apps. During a panel discussion at Nielsen's Consumer 360 Conference in Washington, D.C., in June, IBM's Alberto Jiminez noted, "I would pay a lot of attention to merchant-specific wallets. I know there are lots of apps on people's phones. But the numbers are showing that the growth is at the merchant-specific applications."

Mobile wallet app adoption is imminent, according to participants in the panel discussion. "There's no question it's going to come," said Ben Jankowski, group head, global media, at MasterCard. "One of the barriers to scale is figuring out what the standards are. I think that's a fundamental issue we need to overcome. But there's no doubt adoption will come."

Leveraging Data

To remain profitable in today's economy, merchants of all sizes also need to leverage data and analytics for decision making—and capturing the right customer data is a key component. Merchants will need the right payments products to enable them to gather and analyze data to understand the needs, preferences, and attitudes of specific consumer segments.

Forward-thinking merchants will design offers and make key business decisions using advanced analytics, to ensure products are being marketed to targeted and localized sectors. In addition, data-driven insights can help determine appropriate inventory levels and anticipate changes in customer traffic patterns—to make real-time fulfillment decisions.

Putting It All Together

This year, we've changed the name of our fifth annual directory to better reflect the wide variety of partners eager to do business in the payments space. Our Payment Technology Buyers' Guide features companies with payments offerings in a number of categories, from hardware and software services, to data and analytic tools, to security and risk management products. The staff of ETA and *Transaction Trends* hopes that you will use this guide year-round to meet your payments technology needs.

DATA/ANALYTICS

APRIVA

SECURITY. CONNECTIVITY. MOBILITY.™

Apriva

8501 N. Scottsdale Road, Suite 110
Scottsdale, AZ 85253
877/277-0728
www.apriva.com
Stacey Finley Tappin

Apriva provides secure, end-to-end transaction processing services, including 24/7 customer support. We are connected to over 35 processing platforms, supporting open-loop, closed-loop campus cards, EBT, gift, and loyalty transactions. Apriva supports some 40 devices, plus smartphones and tablets, and currently sells through its ISO/reseller sales channels. Apriva is PCI/PA-DSS compliant. www.apriva.com

HARDWARE OFFERINGS

ePropcessingNetwork

the everywhere Processing Network™

eProcessing Network LLC

1415 North Loop West, Suite 1185
Houston, TX 77008
800/296-4810
www.eProcessingNetwork.com
Steve Sotis

eProcessing Network (ePN) specializes in secure, real-time transaction processing services, solutions, and support for all SMBs. ePN is certified to process electronic payments through all major credit card, check/ACH, and gift card/loyalty processors, selling exclusively through the ISO/reseller sales channels. ePN is PCI/PA-DSS compliant.

RDM®

Transforming Payments

RDM Corporation

619A Kumpf Drive
Waterloo, Ontario N2VK18
Canada
703/286-5734
www.rdmcorp.com
William Buser

RDM is a pioneer in developing and providing multifunctional and network-capable scanners, as well as Cloud-based desktop and mobile remote-deposit capture solutions that allow businesses to remotely deposit checks.

AZT POS

3002 Dow Avenue, Suite 208
Tustin, CA 92780
949/336-6666, Ext. 225
www.aztpos.com
Keddy Chen

ID TECH

10721 Walker Street
Cypress, CA 90630
714/761-6368
www.idtechproducts.com
Jenna West

Red Oak Payment Solutions

12850 Highway 9 North, Suite 600-312
Alpharetta, GA 30004
402/763-9273
www.redoakps.com
Eric Nelson

LOYALTY/REWARDS

♦ Apriva

8501 N. Scottsdale Road, Suite 110
Scottsdale, AZ 85253
877/277-0728
www.apriva.com
Stacey Finley Tappin

Apriva provides secure, end-to-end transaction processing services, including 24/7 customer support. We are connected to over 35 processing platforms, supporting open-loop, closed-loop campus cards, EBT, gift, and loyalty transactions. Apriva supports some 40 devices, plus smartphones and tablets, and currently sells through its ISO/reseller sales channels. Apriva is PCI/PA-DSS compliant. www.apriva.com

Opticard

3260 N. Hayden Road, Suite 204
Scottsdale, AZ 85251
480/538-5511
www.opticard.com
Troy Smith

MARKETING/PROMOTIONS

International Money Transference Conferences

16135 SW 109 Street
Miami, FL 33196
786/238-7857
www.imtconferences.com
Hugo Cuevas-Mohr

Strategic Marketing

13626 S. 32nd Street
Phoenix, AZ 85044
480/706-0816
www.smktg.com
Peggy Olson

SECURITY/RISK MANAGEMENT

♦ Apriva

8501 N. Scottsdale Road, Suite 110
Scottsdale, AZ 85253
877/277-0728
www.apriva.com
Stacey Finley Tappin

Apriva provides secure, end-to-end transaction processing services, including 24/7 customer support. We are connected to over 35 processing platforms, supporting open-loop, closed-loop campus cards, EBT, gift, and loyalty transactions. Apriva supports some 40 devices, plus smartphones and tablets, and currently sells through its ISO/reseller sales channels. Apriva is PCI/PA-DSS compliant. www.apriva.com

♦ Auric Systems International

P.O. Box 458
85 Grove Street
Peterborough, NH 03458
603/924-6079
www.AuricSystems.com
Beth Alpaugh-Cote

Tokenize What Matters™, the AuricVault™ service, is PCI-, HIPAA-, and PII-compliant data storage that securely associates tokens with encrypted data. The encrypted data can be stored, retrieved, updated, and deleted. A permissions system provides secure sharing of sensitive information with third parties while tracking access to the data by user and date/time.

Bluefin Payment Systems

8200 Roberts Drive, Suite 150
Atlanta, GA 30339
800/675-6573
www.bluefin.com
Danielle Duclos

Cimbal Inc.

126 S. Clark Avenue
Los Altos, CA 94024
650/302-2513
www.cimbal.com
Peter Mills

♦ Conformance Technologies LLC

2780 S. Jones Blvd.
Las Vegas, NV 89146
480/629-8808
www.conformancetech.com
Darrel Anderson

Conformance Technologies is a provider of operating systems, educational systems, and expertise used in managing compliance. Solutions include the patented PCI ToolKit®, simplifying merchant PCI compliance; Data Incident Management Program™, which effectively responds to data incidents; Cyber Attack Readiness ToolKit™, providing penetration testing for merchants; and the Data Lifecycle ToolKit™.

Foley & Lardner LLP

90 Park Avenue
New York, NY 10016
212/338-3630
www.foley.com
Stephen Aschettino

PCI Compliance LLC

8547 E. Arapahoe Road, Suite J-201
Greenwood Village, CO 80112
866/949-9777
www.GotPCI.com
PCI-DSS, Mobile App Frameworks, BIDMASTER Programs

♦ Shift4 Corporation

1491 Center Crossing Road
Las Vegas, NV 89144
800/265-5795 or 702/597-2480
www.shift4.com

Shift4 Corporation makes it simple for merchants to securely process credit, debit, and gift card transactions. Its bank- and processor-neutral payment gateway, DOLLARS ON THE NET®, also provides pre- and postsettlement auditing, fraud prevention, EMV, mobile payments, and simplified PCI compliance with security solutions like tokenization and P2PE.

TrustCommerce

9850 Irvine Center Drive
Irvine, CA 92618
949/387-3747
www.trustcommerce.com
Andy Moorhead

SOFTWARE SERVICES

♦ Apriva

8501 N. Scottsdale Road, Suite 110
Scottsdale, AZ 85253
877/277-0728
www.apriva.com
Stacey Finley Tappin

Apriva provides secure, end-to-end transaction processing services, including 24/7 customer support. We are connected to over 35 processing platforms, supporting open-loop, closed-loop campus cards, EBT, gift, and loyalty transactions. Apriva supports some 40 devices, plus smartphones and tablets, and currently sells through its ISO/reseller sales channels. Apriva is PCI/PA-DSS compliant. www.apriva.com

♦ eProcessing Network LLC

1415 North Loop West, Suite 1185
Houston, TX 77008
800/296-4810
www.eProcessingNetwork.com
Steve Sotis

eProcessing Network (ePN) specializes in secure, real-time transaction processing services, solutions, and support for all SMBs. ePN is certified to process electronic payments through all major credit card, check/ACH, and gift card/loyalty processors, selling exclusively through the ISO/reseller sales channels. ePN is PCI/PA-DSS compliant.

♦ Agreement Express

800 - 609 Granville Street
Vancouver, British Columbia V1Y 1G5
Canada
778/877-6444
www.agreementexpress.com
Lana Bukvic

Agreement Express is a SaaS platform that automates the onboarding and underwriting processes for financial services firms. Agreement Express enables organizations of all sizes to provide an incredible customer experience, while collecting and processing infinite amounts of customer data. Global Fortune 500 companies are using Agreement Express every day to grow their businesses.

BridgePay Network Solutions

600 Northlake Blvd., Suite 210
Altamonte Springs, FL 32701
407/960-6441
www.bridgepaynetwork.com
Carlee Hudachko

CardFlight

135 W. 20th Street, Suite 300
New York, NY 10011
800/783-5596
https://cardflight.com/
Natalia Tango

Conformance Technologies LLC

2780 S. Jones Blvd.
Las Vegas, NV 89146
480/629-8808
www.conformancetech.com
Darrel Anderson

FIS Open Test Solutions (Clear2Pay)

3050 S. 35th Street, Suite C
Phoenix, AZ 85034
800/931-0777
www.fisglobal.com
Steve Lacourt

♦ Galitt US

30 S. Wacker Drive, 22nd Floor
Chicago, IL 60606
650/200-7659
www.galitt.us
Gerard de Moura

Galitt has been dedicated for 25 years to providing education, consultancy, testing, and certification services for card-based payment systems. Galitt US is focused on assisting U.S. stakeholders in their EMV migrations with a wide array of services, including off-the-shelf EMV education courses; Brand-qualified test tools; EMV consulting; and certification services.

♦ Net Element Inc.

3363 NE 163rd Street, Suite 705
North Miami Beach, FL 33160
305/507-8808
www.netelement.com
Oleg Firer

Net Element (NASDAQ: NETE) is a global technology-driven group specializing in mobile payments, point-of-sale technology, and value-added transactional services. Among our products you will find Aptito POS system for hospitality, and Unified Payments, one of the leading providers of credit and debit card payment processing services.

NMI

201 Main Street
Roselle, IL 60172
847/352-4850
www.nmi.com
Lisa Puchalski

♦ Payment Alliance International

6060 Dutchmans Lane, Suite 320
Louisville, KY 40205
502/671-4088
www.GoPAI.com
Terri Blain

Payment Alliance International (PAI: www.GoPAI.com) is a leading provider of credit, debit, and prepaid card and check processing solutions, mobile/e-commerce payments, ATM branding, and network and cash management services—all designed to maximize customer success and make business easy. PAI is one of the largest non-bank ATM operators with over 65,000 ATMs nationwide.

♦ PegasusCRM

P.O. Box 33676
404/492-8184
Decatur, GA 30033
www.pegasuscrm.net
Rick Jernigan

PegasusCRM is a customer relationship management tool designed specifically for the retail technology and POS industry. Manage your sales funnel, track your inventory, service your clients, perform administrative tasks, and board your merchants directly to First Data, Vantiv, Transfirst, or any credit card processor within our all-inclusive CRM.

RDM Corporation

619A Kumpf Drive
Waterloo, Ontario N2VK18
Canada
703/286-5734
www.rdmcorp.com
William Buser

♦ Shift4 Corporation

1491 Center Crossing Road
Las Vegas, NV 89144
800/265-5795 or 702/597-2480
www.shift4.com

Shift4 Corporation makes it simple for merchants to securely process credit, debit, and gift card transactions. Its bank- and processor-neutral payment gateway, DOLLARS ON THE NET®, also provides pre- and postsettlement auditing, fraud prevention, EMV, mobile payments, and simplified PCI compliance with security solutions like tokenization and P2PE.

Transaction Network Services

10740 Parkridge Blvd., Suite 100
Reston, VA 20191
703/453-8300
www.tnsi.com
Lisa Shipley

UMS

255 Route 17 South
Hackensack, NJ 07601
201/568-7600
www.unitedmerchant.com
Sean Chung

Wildcard Payments

151 N. Nob Hill Road, Suite 180
Plantation, FL 33324
888/382-8893
www.wildcardpayments.com
Travis Dulaney

Wildcard develops platforms, payment gateways, management applications, and mobile applications supporting the payments marketplace. Our platform supports multiple currencies for card products, mobile payments applications, loyalty programs, and banking functions, allowing secure, real-time transactions for digital and fiat currencies. Wildcard combines traditional validation and authentication strategies with our patent-pending Adaptive Individual Intelligence (AII) system.

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 6th Street NW, Suite 402
Washington, DC 20036
202/828.2635
www.electran.org

ETA CEO
Jason Oxman

Advertising Sales
Alison Bashian
Phone: 703/964-1240 ext. 28
Fax: 703/964-1246
abashian@conferencemanagers.com

Editor
Josephine Rossi

EMV
2.0

Understanding the Payment Fraud Liability Shift

Do you really know who is responsible on October 1?

By Edward A. Marshall and Maayan Lattin

The rollout of the Europay, MasterCard, and Visa (EMV) standard, in which static magnetic-stripe technology is replaced by a computer chip that generates a one-time authorization code, has the potential to significantly reduce counterfeit card fraud at the point of sale. In application, it devalues the data available to bad actors generated in a card-present transaction environment, making it harder to replicate and use counterfeit cards.

To incentivize EMV adoption, the card brands have imposed a liability shift that takes effect Oct. 1, 2015. Despite a push for market education, many merchants—and even certain players within the payments industry—are unfamiliar with the mechanics of that liability shift and the impact it will have on their businesses and partners. This article provides greater insight into the liability shift and explains how a post-October 1 world compares to the pre-October 1 payments environment.

Liability Shift

Prior to Oct. 1, 2015, the financial responsibility for most counterfeit card fraud was borne by the card issuer, usually under the card networks' zero-liability regulations. Merchants that accepted counterfeit cards were generally insulated from liability. Liability assessments to reimburse the issuing banks for their losses were typically borne, if at all, by the merchant from which the card information was extracted (or that merchant's processor), rather than the business accepting the counterfeit card.

Starting in October, however, whichever party in the payments chain lacks EMV-chip technology will be held liable for the expense of any card-present fraud. In other words, the liability will fall on the entity that uses the least up-to-date payments technology.

Once the liability shift goes into effect, every time a fraudulent card-present, or "contact," transaction takes place, there will be a determination of which party—the card issuer or the merchant—should be held responsible for the fraud. The pendulum of fraud liability will swing something like this:

- If a merchant is not EMV certified with a chip-enabled POS terminal, and a customer pays with a chip-enabled card, then the merchant (or its acquirer) will bear the liability for any resulting fraud.
- If the merchant is EMV ready, but the financial institution card issuer has not supplied the customer with a chip-enabled card, the financial institution card issuer will be held liable for the costs of the fraudulent transaction.
- If the merchant is EMV certified with a chip-enabled POS terminal, and the customer pays with a chip-enabled card, and fraud still takes place, the card issuer will be liable. (Much like liability prior to October 1.)

Payment brands, such as Visa and MasterCard, have issued some additional brand-specific guidance for the forthcoming liability shift. Some liability shifts, such as counterfeit fraud liability, lost or stolen liability, and liability for cross-border transactions, will apply only to specific payment networks.

For instance, Visa, MasterCard, and American Express have announced they will not cover counterfeit fraud costs for merchants that are not prepared to process chip cards under the new EMV technology. Of those three companies, Visa is the only brand that will cover "lost or stolen" card fraud, under the same circumstances. That means if a chip card has been stolen, and it is later used and processed as a magnetic-stripe transaction or a chip-and-signature transaction (as opposed to with PIN verification), then MasterCard and American Express will not cover any associated costs from that fraudulent transaction.

Furthermore, merchants are advised to review each payment brand's additional information requirements and guidance because some brands have offered additional incentives to merchants to upgrade their POS terminals to EMV-chip-compliant systems. For example, Visa, through its Technology Innovation Program, has offered eligible merchants PCI DSS-validation waivers if they process 75 percent of their transactions on EMV terminals. Visa also has developed a "safe harbor" for its

Determining Liability for Expense of Card-Present Fraud, as of Oct. 1, 2015

Transaction Type		Counterfeit Liability
Payment Card	POS Terminal	
Chip	Non-chip	Merchant (acquirer) is liable
Non-chip	Chip	Card issuer is liable
Chip	Chip	Card issuer has limited liability*

* Limited liability means that not all instances of chip-on-chip transactions will result in full financial liability on the card issuer. For instance, fallback transactions—where chip-on-chip devices are used but the transaction is not processed using chip technology—will not always result in a card issuer being liable for all costs. The acquirer or merchant must notify the issuer of the fallback transaction and the issuer will only be liable if they approve it.

Merchant Liability by Payment Brand

Payment Brand	Transaction Type	Counterfeit Card Fraud	Lost/Stolen Card Fraud
Visa	Chip-enabled card	Merchant liable	Merchant not liable
MasterCard	Non-chip	Merchant liable	Merchant liable
American Express	POS terminal	Merchant liable	Merchant liable

Global Compromise Recovery Process, which eliminates certain merchant liability when an eligible merchant suffers a security breach.

Merchants and payment acquirers will likely face the most substantial change in this impending liability shift because they have not previously faced the totality of costs associated with payment fraud. Any merchant not certified as EMV compliant by Oct. 1, 2015, could contend with the potentially significant costs of payment fraud. Banks and other financial institutions are issuing new EMV cards in droves, and millions of Americans already have EMV-chip cards in hand. Consequently, starting in October, many of the merchants that have not converted to EMV-chip POS terminals will be exposed to considerable financial risk overnight.

Risk Prevention

Preparing for this liability shift will take some time and planning. For card issuers, EMV compliance requires getting EMV-chip credit and debit cards into the hands of all consumers and educating consumers on the importance of activating and using their new cards. Card issuers and acquirers also must be prepared to field questions and support merchants seeking to fulfill their EMV requirements.

For merchants, EMV compliance requires buying EMV-enabled terminals and meeting the certification requirements for the specific terminal, which may include getting individual approvals from the payment applications and the acquiring bank of each card network. However, once merchants fulfill these requirements, not only will they be EMV compliant, but they also stand to reap other benefits that many payment brands have instituted as additional incentives. In addition, merchants will gain peace of mind from a more secure payment environment.

Of course, EMV technology is a robust security solution, but it will not prevent all data breaches from occurring, nor will it end all counterfeit fraud. EMV will have little impact on e-commerce card-not-present transactions. And while EMV payment systems will make it more difficult for criminals to profit from the information they steal, it is not a complete panacea. Therefore, in addition to upgrading to EMV technologies, merchants should consider implementing point-to-point encryption in their systems and exploring the benefits of tokenization.

Most importantly, however, EMV cards and POS terminals cannot stop the fraud the technology was intended to prevent if updated cards and terminals are not universally implemented throughout the U.S. marketplace. The liability shift was not designed to simply move the responsibility around, but rather to coordinate and encourage all payments players to make the change to EMV systems.

Despite the October 1 deadline, fewer than half of all U.S. merchants are aware of the new technology or the upcoming liability shift. Some 600 million consumers are anticipated to have a new EMV chip card by the end of 2015, yet many still know nothing about the new cards or payments system. Right now, acquirers, ISOs, and card issuers should proactively educate merchants and consumers, instead of waiting for the inevitable ill-fated stories that are sure to teach everyone a lesson, come October. ***TT***

Edward A. Marshall is a partner and co-chair of the payment systems practice group at Arnall Golden Gregory LLP in Atlanta. He also is the founding co-chair of the American Bar Association's Payment Systems Litigation Subcommittee. Maayan Lattin is an associate in the privacy and consumer regulatory practices group at Arnall Golden Gregory LLP in Washington, D.C., and a member of the firm's payment systems practice group.

ADVERTISERS INDEX

EMV 2.0

Matt Pohl

As director of sales support and business development for Integrity Payment Systems, Matt Pohl, ETA CPP, says he and his team of relationship managers are "the lightning rods" for what's happening in the field. His team trains the company's sales force on all procedures and products, including the Europay, MasterCard, and Visa (EMV) standard, which has been a source of "major confusion" for clients in the restaurant vertical in the weeks leading up to the October 1 liability shift.

Does EMV for restaurants involve different considerations than for retail merchants?

There is a vast difference in the investment required on the merchant's part. A restaurant with a stand-alone terminal has a much simpler implementation; however, a large portion of restaurants uses POS software to handle their transactions. A merchant using POS has some tough decisions to make. Some software providers are rewriting their payment modules to include EMV; others will integrate with a third-party gateway or integrate with wireless/ Wi-Fi terminals to facilitate pay-at-the-table. Either way, most restaurants will need to make a considerable investment to upgrade to EMV acceptance.

Are certain locations/patron demographics more compelling for adoption?

I think so. It's important to understand what SIC codes and what areas of the country are more prone to counterfeit/stolen card fraud. Major cities considered "ports of entry" are always high-risk areas for fraud, which makes merchants in these areas good targets for EMV adoption. Also, quick-service restaurants and those using kiosks or other consumer-facing terminals could be at greater risk because there is much less customer/staff interaction at the point of sale to keep the lines moving. Cities with a lot of foreign tourism also are compelling; an influx of EMV cards is to be expected.

Explain some of the "confusion" your team is sorting out with clients.

Restaurants account for the majority of our merchant IDs. Our restaurant merchants are very diverse in terms of size and location—we have many multi million, small ticket establishments and also fine dining establishments in every major city. The majority of our restaurant merchants are smaller mom-and-pop operations.

The main confusion we're seeing involves tip adjustment protocols in restaurants. As of now, there doesn't seem to be any EMV applications that allow for authorization tolerance and tip adjustment after the point of sale. This means restaurant staff need to be retrained on the necessary steps to accept tips. It also creates an awkward situation where a restaurant host or server must ask for the tip amount to enter into their EMV device at the point of sale. Recent news suggests certain platforms are creating EMV applications that will allow for tip adjustment. In general, it seems to be poor timing considering the fast approaching liability shift deadline.

Why are some not adopting EMV?

Some merchants don't want to take on the additional cost right now, others are in denial that they are at risk of credit card fraud and feel the liability shift does not pertain to them. Others may be too stubborn to adapt to new technology. With the evolution of PCI, a lot of merchants recently went through re-terminalizaton efforts due to using "end of life" terminals that were no longer PCI compliant or supported by their processor. Some merchants are wondering when the constant need to upgrade equipment will end.

For those who are, how are they handling the investment?

It seems a majority of merchants are choosing to upgrade, especially merchants using stand-alone terminals. POS software merchants are proving to be more hesitant about upgrading for reasons mentioned above. Additionally, depending on whether their current software provider's solution fits their needs, they may have to purchase a whole new POS system, which is a decision fraught with additional costs and time beyond hardware.

Would PIN protection spur more restaurants to adopt?

It certainly will spur more restaurants to adopt a pay-at-the-table solution, considering you cannot ask a customer for their PIN then walk away to run the sale. Even though PIN entry could be considered the safest procedure to mitigate fraud, it could be more costly to the merchant. It could boil down to how much the merchant can afford to spend on adoption and could lend itself to great opportunities for merchant cash advance providers.

Does a mobile strategy make better sense?

It does, especially once chip and PIN becomes more prevalent. A lot of studies suggest that a mobile POS strategy will be the standard in the future. ***TT*** —*Josephine Rossi*

5 ways we make merchants *happy*

Robust payment software solutions.

1. Intelligent design
2. 5-star support
3. More time with customers
4. Save money on Interchange with level II & III data
5. Understanding they're on the go

PayTrace®
The Secure Advantage

paytrace.com | sales@paytrace.com | (888) 806-6545