January/February 2015

TRANSACTION trends

ETA THE OFFICIAL PUBLICATION OF THE ELECTRONIC TRANSACTIONS ASSOCIATION

countdown TO EMV

Data and insider insight on the U.S. path to compliance

Exclusive:
Read, Learn, and Earn ETA CE Credits
PAGE 20

ALSO INSIDE:

MAGTEK®
SECURITY FROM THE INSIDE

ACTION ITEMS:

- PREVENT DATA BREACHES
- ID COUNTERFEIT CARDS
- STOP FRAUD
- PROTECT OUR BRAND

SELL MORE. SAFER. FASTER. ANYWHERE.

with the DynaPro Family of Products

Recent data breaches make it clear that security and brand protection needs to be at the forefront of Point-of-Sale investments. With the need to future-proof equipment with new EMV requirements, PCI compliance, mobile POS convenience and NFC capabilities, it is important to select the right partner. MagTek has you covered with the most dynamic and flexible solutions and a variety of SDKs.

SUPERIOR TRANSACTION SECURITY

MagneSafe™ Security Architecture • Prevent Data Breaches • Identify Counterfeit Cards • Stop Card Fraud with the Global MagnePrint® Exchange

MULTI-FUNCTIONAL

Secure Magstripe • Signature Capture • EMV Contact/ EMV Contactless • NFC

FLEXIBLE CONNECTIVITY

iOS 30 PIN • Bluetooth 4.0 (BLE) • USB HID • Ethernet

DynaPro

DynaPro Mini

For more information about transaction security and protecting your brand, contact the MagTek Retail Solutions Team at 562-546-6400 | www.magtek.com

1710 Apollo Court I Seal Beach, CA I 90740 I 562-546-6400 I www.magtek.com

contents

The Official Publication of the Electronic Transactions Association Vol. 20 | No. 1

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
John Manasso, Julie Ritzer Ross, Josephine Rossi, and Scott Talbott

Advertising Sales
Linda Baker
Advertising Sales Manager
Phone: 703/964.1240, ext. 13
Fax: 866/466.9187
Lbaker@conferencemanagers.com

Alison Bashian
Phone: 800/335.7500
Fax: 440/232.0398
alisonb@bashian.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.

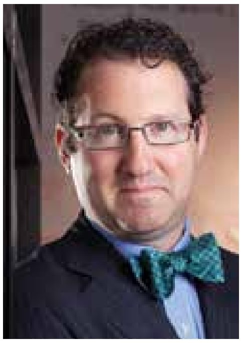
Transaction Trends (ISSN 1939-1595) is the official publication, published six times annually, of the Electronic Transactions Association, 1101 16th St. N.W., Suite 402, Washington, DC 20036; 800/695-5509 or 202/828-2635; 202/828-2639 fax. POSTMASTER: **Send address changes to the address noted above.**

@ETA

Greetings Payments Innovators!

The year is already off to an exciting start for payments, and it's about to get even better: TRANSACT 15, March 31 – April 2 at the Moscone Center in San Francisco, is fast approaching!

TRANSACT 15 is where our industry will collectively determine our future. On the 250,000-square-foot show floor, you will meet the partners who will better your product and attract the customers who will grow your business. You will build influence for your organization, converse with venture capital investors, and step into the media spotlight. You also will be in the front row as the latest technology breakthroughs are debuted.



ETA knows that the future of payments will be decided by TRANSACT's attendees because our annual meetings are where the industry has gathered to make history for 25 years. TRANSACT 15 will be the global payments marketplace with more than 4,000 payments and technology professionals—from established leaders to the smartest disruptors—all coming together in the heart of innovation.

TRANSACT 15 is the must-attend event to access all of the industry's players. Relationships are your best business resource, and TRANSACT is the place to engage current and new partners to do business. Just some of the ETA member companies doing business together: PayPal and Samsung, Apple and the card brands, Vantiv and Mercury, Apriva and GoCoin, First Data and Clover, and so many more. The next great business deal in payments with be made at TRANSACT!

TRANSACT 15 attendees are the future of payments; this is your chance to be part of it! For more information and to register visit www.TRANSACT15.com.

I look forward to seeing you in San Francisco! ***TT***

Sincerely,

Jason Oxman
Chief Executive Officer
Electronic Transactions Association

25 ETA 1990-2015
ELECTRONIC TRANSACTIONS ASSOCIATION
Advancing Payments Technology

YOU'RE IN CHARGE

100% Residuals

or

Upfront Bonuses

NATIONAL MERCHANTS ASSOCIATION
A MERCHANT ACCOUNT THAT WORKS FOR YOU

Simple. Easy. Smart. No Gimmicks.
Maximize your income with your 100% card present, brick-and-mortar merchant accounts. NO volume limits, NO thresholds, NO hidden fees and FREE* POS equipment with EMV, NFC and Apple Pay™ capabilities. A merchant solution that **Works For You**®.

*Free equipment with an annual membership of $79.00.

See us at **Transact15** March 31st–April 2nd

877.810.3032
ProAgentPartner.com

MasterCard To Remove Block on Cuban Transactions

As of March 1, MasterCard will remove the current block on U.S.-issued card transactions in Cuba. The action is based on recent guidance from the U.S. Department of Treasury's Office of Foreign Assets Control that, together with revised regulations issued by the U.S. Department of Commerce, will implement the policies on easing sanctions related to travel, remittances, trade, and banking announced by President Obama in December.

In an online post by Seth Eisen, senior business leader at MasterCard, the company says it will work with its U.S. issuers to support their Cuba-related activities and decisions. Before traveling to Cuba, however, MasterCard suggests U.S. cardholders contact their bank to ensure the card will be supported on the island.

Fraud Plagued Mobile Commerce Channel in 2014

Revenue that mobile commerce merchants lost to fraud spiked 70 percent in 2014 to 1.36 percent, compared to 0.80 percent in 2013, according to LexisNexis Risk Solutions Inc.'s annual True Cost of Fraud Mobile Study. Overall, all merchants lost 0.68 percent of revenue to fraud in 2014 in comparison to 0.51 percent in 2013.

The study was conducted by Javelin Strategy & Research via an online survey using a U.S. retail merchant panel composed of 1,142 risk and fraud decision makers and influencers. In addition, in-depth interviews were conducted with risk and fraud executives at five financial institutions to obtain their perspective on fraud issues.

The complexity of additional payment channels, such as digital wallets, coupled with additional access channels, such as mobile websites and apps, creates more opportunity for fraud, says a study press release. M-commerce merchants accept an average of 4.5 payment channels—significantly more than the 2.6 channels accepted by all merchants—allowing them more fraud exposure than other types of retailers.

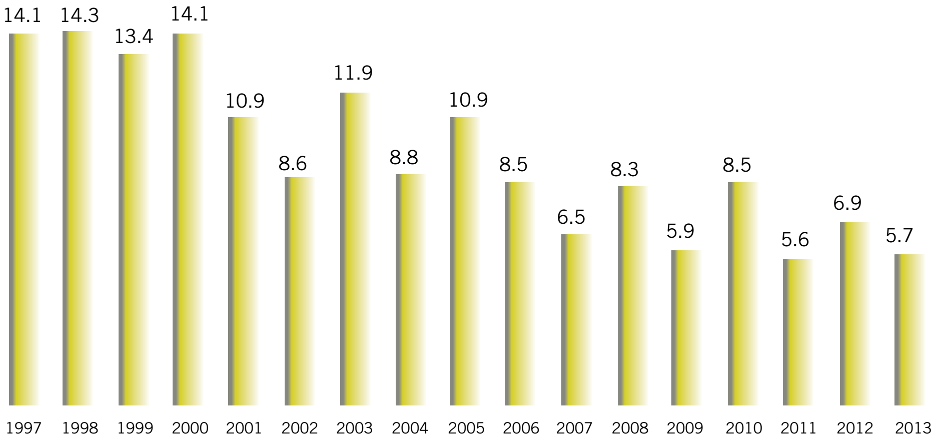
More than one fifth (21 percent) of all fraudulent transactions are attributed to the mobile channel, which is "disturbing due to the fact that the number of transactions occurring through m-commerce channels is still low for the average m-commerce merchant," says the release. In 2014, 14 percent of all transactions were accepted via m-commerce channels.

In addition, the study says merchants are struggling to manage costs for merchandise sold through the mobile channel. The LexisNexis Fraud Multiplier cost for the mobile channel rose to $3.34 in 2014 from $2.83 in 2013, as a result of the expansion of the mobile channel into physical goods markets.

Based on the study results, customer identity verification is the top fraud prevention challenge for m-commerce merchants, followed by friendly fraud. The inability to confidently verify the identity of a customer and his or her device leads to friendly fraud, which is defined as fraud perpetrated by a family member or close associate. The study shows that 24 percent of fraudulent transactions are due to friendly fraud.

Infographic

Acquiring: Monthly Average of New Merchants Per Salesperson, 1997-2013



Note: numbers relate to field sales organization in the small merchant market   Source: First Annapolis Consulting research

Fast Fact

More than **one billion people worldwide—nearly 15 percent of the global population—**will use a tablet in 2015. By 2018, the number of tablet users in the world will reach 1.43 billion.

Source: eMarketer, December 2014

Security 'On the Shelf'

Small organizations are spending significantly more for security than larger organizations yet they aren't fully leveraging the security technologies that they purchase, according to a new study by Trustwave of 172 IT professionals who work for small- to medium-sized businesses.

Twenty-eight percent of organizations are not getting the full value out of their security-related software investments, according to the study. Of the $115 per user that organizations spent on security-related software in 2014, $33 of the investment was either underutilized or never used at all. Researchers conclude that for an organization of 500 users, more than $16,000 in security-related software investments was either partially or completely wasted. One reason why their security-related software sat on the shelf was because IT didn't have the time to implement the software solution properly. Thirty-three percent say they don't have the manpower.

Twenty-eight percent of organizations are not getting the full value out of their security-related software investments.

Respondents also spent significantly more on security-related software, hardware, and services in 2014 than they did in 2013: $115 per user compared to $80, an increase of 44 percent. Moreover, smaller organizations are spending significantly more for security than large enterprise organizations: $157 per user in smaller organizations compared to $73 per user in larger ones.

The study concludes that more organizations will use Cloud-based or managed services this year, as organizations expect a 43 percent increase in such services in 2015.

Retailers Not Ready for EMV

With only nine months until the EMV migration deadline, retail and technology professionals are still unprepared, according to a recent retailer survey by ACI Worldwide that explores EMV readiness, payments security initiatives, and mobile wallets. The survey of 200 retail industry professionals was conducted in January 2015 at the National Retail Federation's 104th Annual Convention and Expo in New York.

The following are highlights from the study:

- Nearly one quarter of respondents are still not fully prepared for the migration to chip and PIN technology, despite the impending October deadline. Of the retailers surveyed (55 percent of total respondents), 14 percent still have work to do, 19 percent are not prepared, and 22 percent are still evaluating their options.
- More than half—59 percent—of respondents say that the past year's data breaches have impacted investments in payment security initiatives. Thirty-nine percent have already increased investments in payment security initiatives, while 20 percent plan to increase investments in payment security initiatives over the next 12 to 24 months.
- Beyond payments security, respondents anticipate their top three biggest investments will be in omnichannel sales/seamless customer experience (37 percent), mobile payments acceptance technology (20 percent), and online/e-commerce initiatives (20 percent).
- Respondents also predict Apple (47 percent) will emerge as the dominant mobile payment technology provider, followed by Google (21 percent), and PayPal (15 percent).

"Data breaches are top-of-mind for retailers, which have already or are planning to increase payment security spending, yet a sizable number of those surveyed are not fully prepared for meeting EMV timelines. At the same time, consumers want assurances that their data will never be compromised when they make purchases," says Lynn Holland, vice president, ACI Worldwide. "Many retailing customers with which we speak to are taking steps to address the EMV requirements, but like any major undertaking, are trying to manage this along with other payment security, IT, and technology initiatives."

ETA'S 2015 ADVOCACY UPDATE

New Year, New Congress

By Scott Talbott

At ETA, advancing your business is our job. As the world's largest payments industry trade association, ETA has created a single industry voice, heard both in Washington and in state capital cities nationwide. ETA's government relations efforts are enormously important to our industry. Federal and state policymakers have a huge impact on how we do business. And this influence is only growing stronger.

In the past year, we have dramatically expanded our government relations activities to meet regulatory and legislative forces. We've registered our first in-house lobbyists, hired new staff, and added new tools to our arsenal with the launch of our political engagement program, ETA Voice of Payments and ETA PAC.

I have had the privilege of leading the ETA Government Relations department during a time of unprecedented change in the payments industry. Now that the 114th Congress has been sworn in, I am pleased to share the highlights of our advocacy program in 2014 in addition to a preview of what may be in store for the payments industry in 2015 and beyond.

Operation Chokepoint

Operation Chokepoint (OCP) is an effort by the Department of Justice (DOJ), Federal Trade Commission (FTC), and Federal Deposit Insurance Corporation (FDIC) to reduce consumer fraud by holding banks and processors liable for the fraud committed by merchants. OCP emerged as a regulator-led effort to target certain types of merchants such as payday lenders, pawn shops, and handgun and ammunition sellers. There was wide concern in the industry, and within those targeted industries, about government overreach and potential impact to lawful participants of the payments system.

ETA tackled this issue with a two-prong strategy to push back on regulators engaged in OCP. We led a group of banking trade associations that raised the alarm about the potential negative economic impacts of OCP and then used its Guidelines on Merchant and ISO Underwriting and Risk Monitoring as a model on how the industry can be a partner to law enforcement instead of an adversary.

As a result of these efforts, the DOJ, FTC, and FDIC have taken a number of steps to slow and reduce OCP, including removing the list of targeted industries, opening internal investigations, and curtailing public comments. While we can't yet claim mission accomplished, we can say ETA's efforts have had a very positive effect on scaling back OCP.

Data Breaches

With a string of high-profile data breaches hitting consumers in the past year, data breach and security is a key issue for ETA. Congress held more than a dozen hearings on the topic, and the issue of data security will be a priority for legislative action in the 114th Congress. Currently, there are 48 different state laws that detail what a company must do to notify customers if it is the victim of a data breach. During 2014, Congress was working toward enacting legislation to create one uniform national standard for data breach notification.

Given the interconnected economy and payments system, most ETA members operate in multiple states. ETA strongly supports the creation of a preemptive uniform national standard for breach notification. The president recently called for data breach legislation as part of his BuySecure initiative, and we are optimistic that Congress will take this issue up in 2015.

Information Sharing

Frequently, a payments company or government agency will obtain information about a cyber attack, which can be the result of an attack on the company or as part of an investigation. It would be beneficial to the industry to share threat information with others in the industry or the federal government. Currently, a number of existing laws prevent this type of information from being shared. Allowing the information to be shared will bolster industry defenses to cyber intrusions and allow entities to potentially limit or stop at attack from taking place.

ETA contends that liability protection and special carve-outs from existing laws to allow companies and the government to share information about cyber threats will lead to increased cyber threat preparedness.

During 2014, ETA:

- submitted testimony to several congressional committees that focused on the issue
- met with congressional offices and federal regulators
- pushed ETA's positions in the media, including op-eds in national publications.

During the State of the Union Address on January 20, President Obama proposed streamlining the ways in which private businesses and the government work together to prevent breaches. Congress appears to be in agreement with the president, so we are hopeful that we will see legislation this year.

Prepaid Card Regulation

In addition to the U.S. Congress, federal and state regulatory bodies have the ability to dictate policy that can greatly impact the payments industry. During 2014, ETA engaged with federal and state regulators to advance the payments industry's positions.

The Consumer Financial Protection Bureau (CFPB) has released an 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 create confusion for consumers with disclosure requirements. The proposal also includes peer-to-peer payments, mobile wallet solutions, and digital currency.

ETA's position is that over-regulating the prepaid card and emerging payment industry could reduce consumer choice and stall innovative features that benefit consumers. We are working with Congress and the CFPB to express our concerns about the breadth and depth of the proposed burdens. Additionally, we took the following steps:

- hosted a lunch-and-learn for 35 congressional staff members to educate them on the role of prepaid cards
- met with the relevant congressional committees to discuss our concerns
- created a working group to file a formal comment letter with the CFPB
- met with the staff of the CFPB.

The CFPB's comment period is open until March 23, 2015. We expect to see a final rule on regulation of prepaid cards in the middle of the year.

Outlook for 2015

Now that 2015 is underway, ETA continues to expand its advocacy efforts and focus on the following federal and state legislative and regulatory issues: pushing back on OCP and advancing a data breach notification standard, cyber info sharing, tax reporting, and many state issues. In addition to direct advocacy, we will host topical Policy Days in D.C., as well as Regional Policy Days around the country.

Politics is not a spectator sport, so we encourage you to get involved with ETA as its represents the payments industry. Our new political engagement program, ETA Voice of Payments, gives you the tools necessary to ensure elected officials hear the voices of their constituents on issues of importance to the $5 trillion payment processing industry. Please visit http://voiceofpayments.org and start participating today. ***TT***

Scott Talbot is senior vice president of government affairs for ETA. Reach him at stalbott@electran.org. For more information, contact Jaime Graham, senior manager of government affairs, or Grant Carlson, government affairs coordinator, at 202/828.2635.

COUNTDOWN TO EMV

Lessons L

The latest research and data from EMV early adopters point to problems ahead for U.S. migration

By John Manasso

As the United States embarks on the migration to Europay/MasterCard/Visa (EMV) in October 2015, it faces a far more daunting task than some other nations that have made the migration over the past decade.

Countries that have managed their migrations in as seamless of a manner as possible generally have done so with government-backed, high-profile education campaigns. Those countries also tend to have had fairly consolidated banking industries.

In the United States, banks and industry groups are tackling the education challenge, and recent studies show gaps in the result. One out of every three small merchants has not heard of the coming migration to EMV, according to a survey conducted by the Aite Group, an independent research and advisory firm.

Other research has found similar results. In a November 2013 survey of "small and micro merchants," 20 percent said that they would be EMV-capable within the next 12 months while 50 percent had "little to no knowledge" of the EMV liability shift, according to Javelin Research and Strategy, an independent payments industry research and strategy group.

The second component that will complicate the U.S. migration is the large and varied banking landscape of the world's largest economy. The United States has 8,000 banks and 4,000 credit unions, and the variety of payment options available serves to fragment the market. (Research shows that the EMV migration on debit will lag that of credit in part because of the Durbin Amendment, which mandated that a debit card must be able to be processed on at least two unaffiliated networks.)

Compare the United States to Australia, with a population of 22.7 million (roughly one-fourteenth the size of the United States' 317 million people). Australia is dominated by four large banks and has about has 100 credit unions. In three months, the country had converted 80 percent of its POS terminals, according to Lance Blockley, managing director of RFi Consulting, a firm specializing in payments, who managed Australia's migration to EMV.

earned

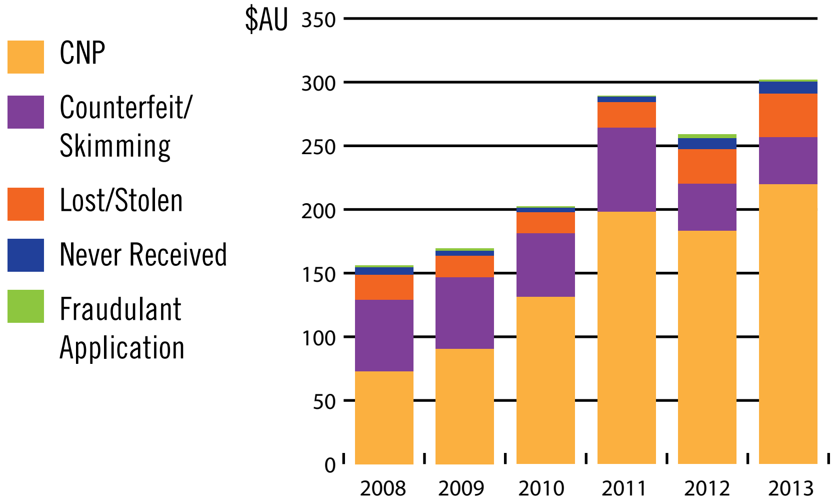
"Part of the fragmentation is the sheer number of banks when it comes to regional banks, community banks, credit unions, and so on," says Nick Holland, retail payments practice lead at Javelin Strategy, of the United States' coming challenge. "It's not to say they won't be proactive in this as well, but certainly you want very coherent messaging in terms of what is required from merchants and consumers, and it just doesn't seem to be being put out there."

Tales From Down Under

One of the reasons why education is an integral part of the migration process is that consumers must be made aware of the slight changes when making purchases. After years of swiping their magnetic-stripe cards, they will need to acclimate to using a card reader that takes in all or part of the card to read the chip, similar to many ATM machines.

The first EMV cards were issued in Australia in 2003, and by 2007 one million were in circulation, according to the Aite Group. (The country has 8 million cardholders.) Initially, Australia allowed "chip and signature" (which is what the United States will do) with a voluntary PIN. A drawback of chip and signature is that it does not cut down on stolen/counterfeit cards because a fraudster can forge a signature.

Fraud Loss on Australian Cards



Source: Australian Payments Clearing Association, "Australian Payments Fraud Details and Data," 2014
Note: numbers are in $AU millions

In August 2014, Australia eliminated signature and migrated to a system that only used "chip and PIN" to cut down on stolen/counterfeit fraud. The announcement was made in January 2014 and by October 2014, transactions made without a PIN were rejected. In the weeks leading up to the change, the industry and government undertook a massive public relations and advertising campaign entitled "No PIN, No Pay." Every day major newspapers ran full-page ads of the countdown under the "No PIN, No Pay" slogan.

It was partly a scare campaign, and it worked: The country had 83 percent PIN use in July and 95 percent by August, says Blockley.

[In the United States, the rollout will be much slower. The expectation is that by the end of 2015, 29 percent of all credit cards (or 166 million) and 17 percent of all debit and prepaid cards (or 105 million) will be EMV, according to Javelin's report.]

"We had next to no reports of people being held up at the checkout," Blockley says of Australia's migration. "There was nothing on 'Today Tonight' or 'A Current Affair' [the country's leading television news programs] or TV shows that might scandalize things, and in October when we were actually rejecting transactions that [didn't] have a PIN, the level of rejection across the banks [was] absolutely minimal. Effectively, we have managed to move the whole of the card base to using PIN."

Because EMV will make a major impact on lost/stolen fraud, fraudsters already have undertaken their own migration to other types. Fraudulent application fraud (the use of fraudulent identities to apply for cards) went from $1.1 million Australian in each of 2010 and 2011 to $3.5 million in 2012, according to Australian Payments Clearing Association (APCA).

However, the biggest jump in the kind of fraud associated with EMV is card-not-present (CNP), since the technology is not designed to prevent this kind of fraud. CNP fraud in Australia rose from $72.8 million in 2008 to $90.6 million in 2009 to $131.2 million in 2010 to $198.1 million in 2011 before dipping to $183.1 in 2012, according to the APCA. In 2012, merchants and issuers began to use increased tools and analytics, such as 3-D Secure, which adds an extra layer of security to the transaction, to prevent CNP fraud. MasterCard required 3-D Secure for online purchases more than $200 Australian, and Visa requires that all cards enroll in Verified by Visa. 3-D Secure is a program that the major card brands have made available to issuing banks and for which cardholders can register. It includes the three- or four-digit CVV/CVC code, which can never be printed or stored following a transaction, and increases the chance that a transaction will be approved because of the higher level of authentication it provides.

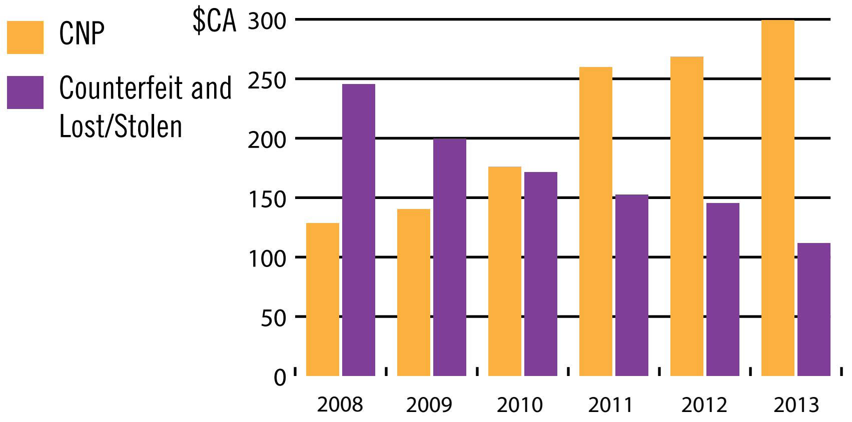
Experiences Across the Pond

The United Kingdom made its transition to EMV long before Australia did (2003 to 2005), and it also employed a large campaign, which, like Australia's, included a healthy dose of government involvement. The campaign was dubbed “I HEART PIN” and included billboards, television ads, a tour of retail malls, and regular progress reports on cardholders and EMV statistics. The entire migration, including cards and terminals, took a single year, from January 2004 through the end of December. The liability shift took place in January 2005.

It began with a small pilot program in the city of Northampton, involving 600 merchants and 180,000 cards, according to Aite Group. At the time of the U.K. migration, fraud rates were 14 basis points, compared to 5 basis points in the United States at the same time.

“I do think that the U.K. was one of the best migrations that we’ve seen,” says Julie Conroy, research director at Aite Group and the author of that report, “and I think largely that was because the issuers were bleeding, so they were highly motivated but also you had strong government support.”

Fraud Loss on Canadian Credit Cards



Source: Aite Group, “EMV: Lessons Learned and the U.S. Outlook,” 2014
Note: numbers are in $CA millions

The impact that the U.K. migration had on overall fraud was profound. In 2005, counterfeit fraud represented £97 million. That fell to £43 million in 2013, as reported by Financial Fraud Action UK. In 2005, lost/stolen fraud accounted for £89 million, which fell to £59 million in 2013.

As the United Kingdom ranked among the first countries to move to EMV, it also is where the trend of shifting fraud type after EMV implementation first began. While CNP fraud represented £183 million in 2005, it leaped to £328 million by 2008.

One factor that is important to note here is the simultaneous growth in e-commerce during this period. While the aggregate numbers of CNP, counterfeit, and lost/stolen fraud grew by £34 million during an eight-year period, it actually represents a dramatic overall reduction not just in annualized terms but also when considering the growth of e-commerce over the total time frame.

“The perceived wisdom [is] that EMV was the cause of this big spike in card-not-present fraud…we’ll say it was contributory, and certainly what’s never been taken into account is the massive growth of e-commerce as well,” says Holland. “So what you had was fraud increasing, yes, but as a fairly constant percentage of the overall online transactions that were happening.”

While it was “expedient” to say that CNP fraud will spike when a country undertakes an EMV migration, Holland believes the United States will be different because CNP fraud already is taking place in substantial numbers.

“We’ve modeled EMV—whether it comes in or not—will absolutely do nothing when it comes, positively or negatively,” Holland says. “Card-not-present [fraud] is going to grow irrespective.”

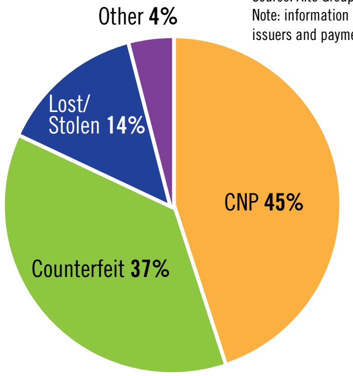
Elsewhere Around the World

In other countries, lessons can be drawn for the United States’ coming migration. For example, some U.S. merchants prefer a quicker, more streamlined e-commerce experience for their customers, which can result in an increased willingness to accept fraud, according to Randy

Fraud Loss on U.K. Cards

	Before/During EMV Migration			After EMV Migration							
	2003	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**
Remote Purchase (CNP)	£122.1	£150.8	£183.2	£212.5	£290.5	£328.4	£266.4	£226.9	£220.9	£246.0	£301.1
Counterfeit	110.6	129.7	96.8	98.6	144.3	169.8	80.9	47.6	36.1	42.1	43.4
Lost/Stolen	112.4	114.4	89.0	68.5	56.2	54.1	47.7	44.4	50.1	55.2	58.9
Card ID Theft	30.2	36.9	30.5	31.9	34.1	47.4	38.2	38.1	22.5	32.2	36.7
Mail Non-Receipt	45.1	72.9	40.0	15.4	10.2	10.2	6.9	8.4	11.3	12.8	10.4

Source: Financial Fraud Action UK, “Fraud the Facts 2014”
Note: numbers are in £GBP millions



Current U.S. Card Fraud

Source: Aite Group, "EMV: Lessons Learned and the U.S. Outlook," 2014
Note: information gathered from Aite Group interviews with card executives from 18 of the top 40 U.S. issuers and payment networks, April and May 2014

Vanderhoof, executive director of the Smart Card Alliance.

When Mexico migrated to EMV between 2005 and 2009, CNP fraud quickly became a challenge. As a result, the Mexican government issued a directive, suggesting the use of 3-D Secure, which the country's banks took as a mandate. That has successfully cut the country's CNP fraud rate, according to Aite Group.

In Canada, the shift to EMV was announced by the card brands and the country's leading debit network, each on their own timetables, between 2003 and 2005. The liability shift initially was set as October 2010 but was pushed back to March 2011. The debit network, Interac, announced that as of December 2012 issuers were subject to fines if any of their debit portfolio was not EMV-enabled.

Again, with Canada's migration came a change in fraud type. In 2008, counterfeit and lost/stolen represented a $245.4 million Canadian Dollar problem while CNP was $128.4 million, according to data from Canadian Bankers Association and cited by Aite Group. They equaled each other in 2010 (roughly $170 million Canadian apiece), and by 2013, CNP fraud rose to $299.4 million Canadian while counterfeit and lost/stolen fraud fell to $111.5 million.

New Habits in the United States

While CNP fraud grew only after EMV migrations in other countries, it already is on the increase in the United States. Aite Group estimates it represents 16 percent of total fraud but that might only be a starting point. Already, CNP is the largest category of merchant losses, totaling $1.92 billion, according to a 2012 report by Nilson, and CNP also is growing faster than counterfeit fraud, according to FICO, the business and software analytics company (both statistics were cited in a February 2014 white paper by the Smart Card Alliance). CNP fraud is expected to be 1.7 times greater than POS card fraud in 2014 and almost four times more in 2018, Javelin predicts.

Entering into this new environment, merchants will have to take additional steps to protect themselves for CNP transactions. The most common is to use the three- or four-digit security code on the back of the card. Adding this step creates more friction during the online checkout process and, as a result, some merchants elect to forego it. That might not be such a viable choice anymore. Once a customer has an EMV-enabled card, liability for such fraud will shift to the merchant instead of the issuer as of the October 2015 deadline.

"Part of the reason for that is merchants see abandonment of shopping cart whenever they try to ask for additional info from the customer," says Vanderhoof. "Merchants who are anxious to capture every sale possible are willing to assume some risk and may take some bad transactions in order to get more good transactions. It's a risk decision that merchants play all the time, where they balance the desire to increase sales with desire to increase fraud risk."

Another tactic is for merchants to subscribe to databases known as security address verification services. These attempt to match the address given by the purchaser to other known information about the cardholder through available sources. A flaw with these services is that a cardholder's address can be found on social media and fraudsters can use that to their advantage to circumvent the tool.

Other merchants use "device signature" services that compare the IP address of the purchaser to ensure it is in the same country as those of the cardholder.

Experts say that merchants' best defenses against CNP fraud might be tokenization and encryption solutions, some of which are sold by data security firms and some of which already are bundled into the menu of options that processors offer. A "layered" approach, including possibly several of these options, could be best, Holland says.

The change to EMV will affect merchants but also customers. Holland has heard of cases in which consumers, ignorant of the new procedures, have wrestled with POS terminals to get their cards out and broken the terminal in the process.

While that represents an extreme example, the reality is during the transition, checkout procedures—regardless of whether in a brick-and-mortar store or online—could become lengthier, and that could have implications for merchants. Holland says the potential increase in actual transaction time at the point of sale could represent a "fairly large latent threat." Metrics exist for the largest retailers like Wal-Mart that indicate the amount it costs them when customers spend extra time at the point of sale, he said. The best-case scenarios will add a few more seconds per transaction.

Holland then described the worst-case scenario.

"With people not knowing what to do and confused and the clerks at the checkout having to train people how to use their EMV card, if it's every other person in line, you could be adding minutes per transaction and that has a huge material impact," he says, "because you have scenarios with clearly greater lines of a checkout and quite literal cart abandonment where people drop their carts and can't be bothered anymore."

Nine months remain to help sort out such potential issues. ***TT***

John Manasso is a contributing writer to Transaction Trends. *Reach him at john_manasso@yahoo.com.*

HCE, EMV, and NFC: The Perfect Convergence Storm?

POS business as usual is over, that's for sure. But forecasting what's next isn't as clear

By Julie Ritzer Ross

A "coming together from different directions." A "gradual change of a number of things…to become similar or develop something in common." That's how the *Oxford English Dictionary* defines the word "convergence." The term does not refer specifically to payments—but it does apply to the payments industry. Why? A convergence of host card emulation (HCE), Europay/MasterCard/Visa (EMV)-enabled POS technology, and near-field communication (NFC) is said to be occurring. And, fanning the flames are new solutions that adhere to the EMV standard and accommodate chip-and-PIN and/or chip-and-signature payments, along with HCE, a technology that mirrors NFC function in the Cloud, allows NFC-based applications to operate without a secure element and trusted service managers, and eliminates the need for issuers to conform to card provisioning restrictions.

"It's almost a perfect storm now," says Pascal Caillon, general manager, North America for Proxama, a provider of mobile proximity marketing, mobile wallet, and payment solutions. "EMV migration will help to resolve the contactless (NFC) acceptance issue…and HCE to enable issuers to permit NFC payments on the Android smartphone base."

Transaction Trends discussed convergence and its implications with Caillon and several other solution providers, along with ISOs, payment processors, and industry consultants.

TRANSACTION TRENDS: By most estimates, only 220,000 of the 9 million merchants in the United States have enabled their POS systems to accept payments via NFC. Why and how are HCE and EMV catalysts for further NFC adoption?

"…ONE IN 10 IPHONE 6 OWNERS IN THE UNITED STATES HAS ALREADY USED APPLEPAY. THIS RATE IS EXPECTED TO INCREASE SIGNIFICANTLY…"

—Bob Graham, Virtusa

KAREN COX, vice president, payments and retail solutions, Moneris Solutions Corp.: EMV and reducing counterfeit card fraud in face-to-face transactions are the fundamental drivers for merchants in upgrading POS technology. EMV adoption will, by default, encourage NFC adoption as contactless capability is built into most modern, EMV-capable PIN pads and POS terminals.

HCE will also help to spur NFC adoption—although it will not be the sole catalyst. NFC has been around for quite some time, but solutions like ApplePay are aiding awareness of HCE. Generally speaking, HCE bypasses the need to use the secure element controlled by the carriers for card credentials—and it simplifies distribution. However, HCE solutions will still use EMV at the POS level because the app with the credit information will have to be EMV-compliant.

BOB GRAHAM, senior vice president, banking and financial services, strategic business development, Virtusa (a global information technology services consultancy): EMV and HCE will contribute to NFC adoption, but more so from the EMV side. Last year, Google announced support for HCE in Android KitKat 4.4, which became a big part of its Google Wallet initiative. But, adoption rates were dismal. Merchants saw little reason to spend the money to deploy NFC-enabled POS terminals because consumer demand for NFC capability was essentially non existent.

But two major EMV-related things have happened to change the playing field in the U.S. market as far as NFC is concerned. One is the October 2015 EMV liability shift, when liability for fraudulent card-present transactions will become the responsibility of merchants if they are not using EMV-enabled POS terminals. This certainly gives merchants a financial impetus to upgrade their equipment, and it is likely that their new terminals will have contact EMV and contactless NFC capabilities.

The other development is the launch of the iPhone 6 with ApplePay NFC-enabled mobile wallet technology, which utilizes industry-standard EMV contactless protocols over NFC. Just recently, InfoScout [a provider of real-time insight into shopping behavior] reported that one in 10 iPhone 6 owners in the United States has already used ApplePay. This rate is expected to increase significantly as consumers further understand the capabilities—and as more merchants deploy NFC-enabled POS equipment.

As for HCE…the cost of directly managing the secure element on multiple manufacturers' devices has largely inhibited any level of adoption from issuers, and merchants have shown little appetite to spend on new POS terminals. HCE unlocks the potential for NFC applications without the need for integration with mobile devices' secure elements or for the support of a trusted service manager. Applications can be provisioned directly to virtual secure elements without any third-party [device manufacturer] involvement.

PATTY WALTERS, senior vice president, corporate EMV strategy, Vantiv (a payment processor and solutions provider): Enabling technology applications like HCE will also help adoption because they offer merchants an option to cater to consumer demand by expanding the omnichannel experience at the point of sale. Card authentication improvements associated with EMV give retailers the ability to prevent counterfeit fraud during checkout. Both typically require the use of payment terminals or tablets—which are now fully enabled with NFC as a standard feature.

TRANSACTION TRENDS: Still, the industry consensus is that NFC deployment will be gradual. Why?

CAILLON: HCE is currently available only on the Android operating system. When it becomes available on the Windows and BlackBerry operating systems, it will become more of a driving force around NFC adoption.

MARK CASTRECHINI, vice president, product management, Merchant Warehouse: EMV requires a computer chip and secure element, meaning that mobile wallets could certainly perform the same EMV functions as contactless EMV cards. For this reason, mobile application developers could consider EMV functionality in their products. Enabling a mobile wallet application to perform an EMV transaction is unlikely to significantly accelerate NFC adoption because, as early indicators show, consumers—although interested in and willing to try the new technology—are not heavily adopting mobile wallets unless there is a compelling value-add to their use. However, as more new unique mobile wallet applications hit the market, it will be in developers' best interests to support a multitude of payment technologies, including NFC driven by EMV.

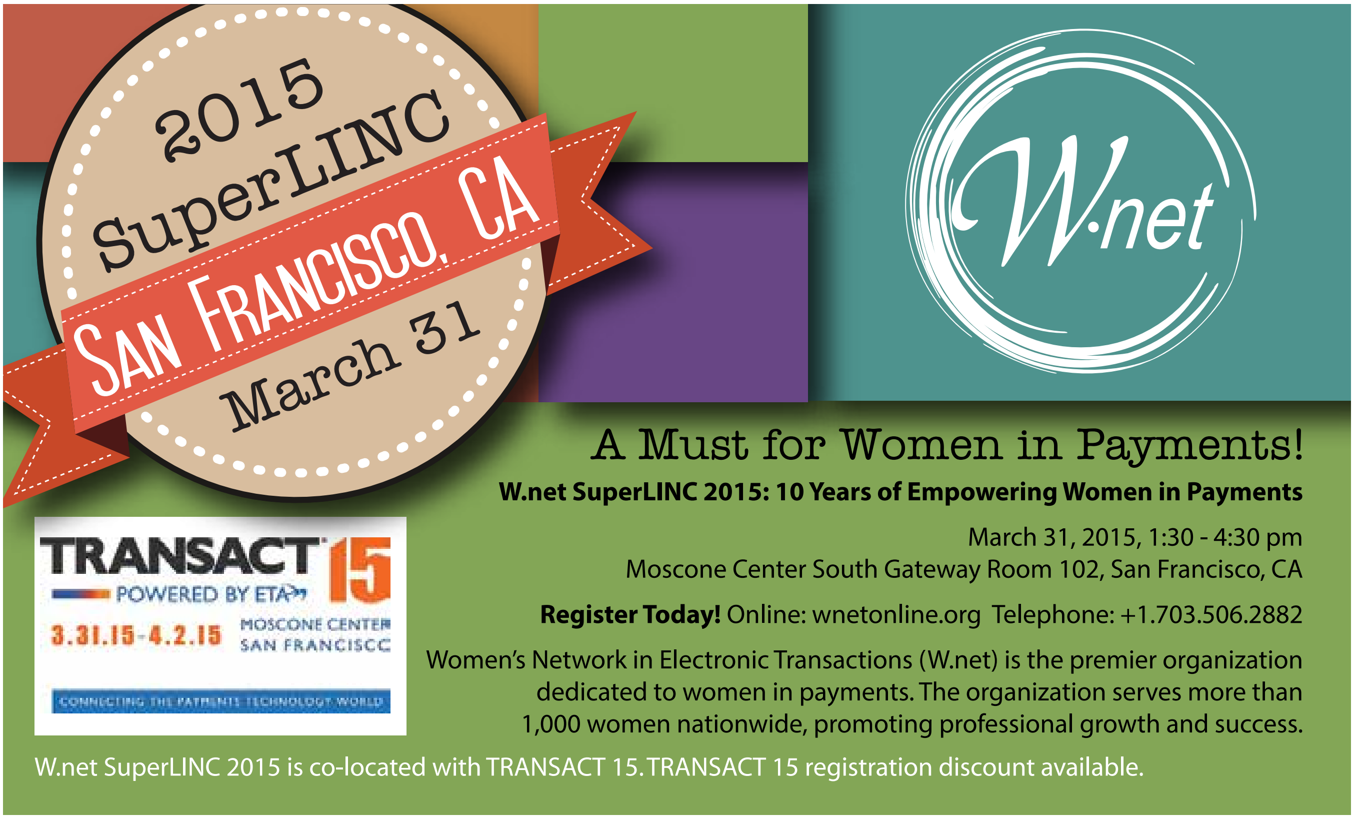
MIKE NOURIE, Boston-based security expert: Unfortunately for mobile payments users, NFC will only be an option with contactless EMV card readers. Therefore, adoption will happen at a much slower rate than on the nonmobile side.

"...WE WILL SEE THE EVOLUTION OF THE CONTACTLESS CHECK-OUT EXPERIENCE LAST WELL INTO 2017 AND BEYOND."

—Patty Walters, Vantiv

WALTERS: Many merchants are behind the EMV implementation curve and may choose to enable new payment options later, meaning we will see the evolution of the contactless checkout experience last well into 2017 and beyond.

TRANSACTION TRENDS: Some say HCE is strong enough to support the security needed for NFC, or that it is fast becoming so. What's the rationale behind that assertion?



CASTRECHINI: While HCE was developed primarily to solve the challenges of localized secure elements, it was designed with NFC security in mind. In fact, through various security mechanisms—such as tokenization—HCE offers a significant improvement over legacy card acceptance mechanisms that are currently in use, like magstripe readers.

COX: HCE does not require the use of the secure element for card credentials, but bypassing the secure element does not make it insecure. HCE is strong enough in that it leverages Cloud-based and other trusted secure environments for credential management. The transactions themselves include the EMV security found in card-based NFC transactions. This can include tokenization to replace the real card data.

"HCE IS MORE SECURE ONLY IF IT IS DONE RIGHT—AND NOT STORED IN THE MEMORY OR OPERATING SYSTEM OF THE SMARTPHONE."

—Barry Mosteller, CPI Card Group

GRAHAM: Since Google announced support for HCE in the Android KitKat 4.4 operating system last year, there has been much debate about its [HCE's] security risks—around the vulnerability of the Android operating system to hacking and other forms of malware, and the reliance of HCE on maintaining connectivity with the Cloud. However, issuers and the card networks have worked on addressing these problems through scheme mandates, like single-use keys. Card data are now stored on the Cloud, not on devices, and tokens are either used once or in limited-use mode. Consequently, the current thought is that it would take considerable effort to hack into HCE-based mobile payment data—and for a limited return given current tokenization schemes.

TRANSACTION TRENDS: Other observers say that HCE does not adequately support NFC on the security side. Why not, and/or what will change this?

NISH MODI, senior vice president, product and innovation, SecureNet (an end-to-end payments processor): HCE overall is considered by some security experts to be less secure than hardware. However, additional security layers and strategies—such as white-box cryptography, obfuscation of key data, and securing the communication channels between the device and server with encryption—can be added to HCE-based mobile payments.

BARRY MOSTELLER, director, research and development, CPI Card Group (a producer of financial and EMV chip cards): HCE is more secure only if it is done right—and not stored in the memory or operating system of the smartphone. Not all HCE is created equal; it has to involve the Cloud. A phone can be hacked much more easily than the Cloud, but Cloud-based HCE behind an encrypted firewall is fairly secure.

NOURIE: The purpose of a secure element is to provide a secure chip that houses only the payment information and is separate from the phone's hard drive, securing it from the rest of the mobile device. The secure element ensures that only the payment terminal is able to read the payment information. Otherwise, if the device is stolen, the would-be thief would be able to more easily access the payment information. I think the only true way to ensure that payment information is secure is to encrypt it in a separate chip designed to work separately from the mobile device.

ED PAGE, managing director, Protiviti (a global financial, technology, operations, and governance consulting firm): Tokenization provided by HCE represents a major step forward in terms of HCE and securing NFC, but it is not and never will be a silver bullet. Biometrics, along with location-based verification and transaction pattern detection software solutions, needs to play a part as well.

WALTERS: HCE security will continue to evolve as the HCE standard does. We can anticipate a day when we will have many layers of security to protect the payment information stored and communicated in the Cloud, and many will look very similar to security layers we use today. One-time-use tokens, real-time analysis, and multifactor authentication—think fingerprints—are all components that will establish a secure HCE model of the future.

TRANSACTION TRENDS: Could enhanced security from EMV cards mitigate consumers' security concerns and keep them from moving over to mobile payments?

BOB LEGTERS, senior vice president, payment products, North American Retail Payments Group, FIS (a provider of banking and payments technology solu-

tions, financial/payments consulting services, and outsourcing solutions): A lot of it is going to depend on what payment methodologies retailers accept. And there is the reality that nothing is 100 percent secure—so consumers are not going to run away from cards in droves.

KIRK NOSWORTHY, CIO, State Enterprise Solutions, Xerox (which offers payment processing and collection services in addition to POS hardware): There is no expectation that consumers are about to give up using their credit cards. We see the demand in the U.S. being driven by consumers who will still want the new EMV cards for better security and merchants that wish to reduce the incidence of fraud.

MOSTELLER: I think consumers will continue to use cards. EMV does point of sale very well. That's why it was built—to secure transactions at the point of sale. EMV does not help with card-not-present. Although it devalues data, it does not stop a data breach.

VAUGHN ROWSELL, CEO, Vend (a provider of Cloud-based POS and retail management software): Consumers want a payments solution that is secure, easy to use, and widely accepted. However, these factors will not compel them to accept mobile payments over EMV, because the lure of mobile payments is about more than just security.

Consumers will adopt mobile payments because they are secure, and because their features and functionality are superior to those of credit cards. Mobile payments yield better analytics capabilities and, hence, the potential to receive targeted, mobile-based, context-aware capabilities and offers. A credit card that is disconnected from the Cloud simply cannot provide those benefits.

EMV simply makes the existing, outdated technology more secure. It does not add targeted, mobile-based, contextually aware functionality to payments—and that functionality is what will encourage consumer adoption.

WALTERS: EMV has the power to quell consumer concerns about losing card payment data—but only until the first compromise requires that EMV chip cards be reissued because of online fraud.

Still, in the end, EMV spells the conclusion of our business-as-usual experience at the checkout and welcomes the U.S. consumer into a new world of payment options. ***TT***

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

Making Mobile Payments Work for Merchants

To create a profitable and secure mPOS solution, merchants must consider several factors

For years, Starbucks has been the merchant poster child for mobile payments acceptance. However, with advances in technology, businesses no longer need to be publicly traded with a market capitalization of $60 billion to leverage cutting-edge mobile payments solutions. Software companies can access Big Data and innovative app designers can either white-label their services or customize them, enabling small- and medium-sized businesses to have easier and cheaper access to mobile payments.

Still, merchants need to undertake a measure of self-analysis before deciding if their customer base is the kind that would adapt to mobile payments and deploying a mobile point-of-sale (mPOS) solution. If a merchant decides that mobile payments are the way to go, it can look forward to a lower total cost of ownership (of mPOS), better portability and greater ease of use, more flexible software options for managing its business, and better user interfaces that offer expanded capabilities.

The information in this summary is intended for ISOs, acquirers, and payments facilitators to use when helping their merchant clients evaluate options for mPOS solutions.

Market and Business Models

Not surprising, mobile device use is on the rise in the United States: 58 percent of U.S. adults own a smartphone, and 42 percent own a tablet. Even among lower-income demographics, smartphone use remains high, with ownership rates of 53 percent for households that earn between $30,000 and $49,999 and 47 percent for those earning less than $30,000. Moreover, 30 percent of consumers use the mobile phone to make decisions about retail visits.

For merchants, evaluating their own customers is crucial. Factors that correlate with high mobile phone ownership and usage include average customer age and household income. In addition to a merchant's own observations and internal data, outside data resources are available. The Pew Research Center Internet Project offers a Mobile Technology Fact Sheet, and Google Shopper Marketing Agency Council and M/A/R/C Research are among those who make such information available publicly.

Another key consideration is the merchandising environment. Does the merchant offer the kinds of products and services that work well with mobile payments (per-

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 www.electran.org/cpp for a link to the quiz to test your knowledge and earn 2 ETA CPP CE credits per quiz!

haps an ice cream shop would rank among the ideal ones while a mattress store, with its high-ticket cost, would not)?

Other factors that a merchant must contemplate include its budget for upgrading, the percent of customers who might use mobile payments, whether its customers would use loyalty programs, and whether it is financially feasible for the merchant to offer such discounts. It's also important to consider what additional security procedures would be needed to deploy the mPOS solution effectively.

The Mobile Payment Ecosystem

While business owners know most of the providers and stakeholders in the mobile payments world, they must familiarize themselves with new stakeholders that factor into the decision-making process.

The following mobile payment mechanisms and technologies are either currently in use or on the horizon, according to experts, for customer payments:

Chip. A small piece of semiconducting material (usually silicon) embedded with an integrated circuit (IC). Mobile phones contain IC chips, and payment applications can be managed on these IC chips.

EMV (Europay/MasterCard/Visa). A global standard for interoperation of IC cards and compatible mPOS and POS terminals and ATMs, to authenticate credit and debit card transactions.

Contactless. Proximity-based wireless technology that enables payment transactions via chips embedded in payment cards, tags, and mobile phones. Near-field communications (NFC) technology is an industry-leading contactless standard.

Mobile coupon. Usually these digital coupons are sent to the consumer's mobile device and are redeemed at the merchant POS directly from the device. Mobile coupons can be part of a loyalty program to reward and encourage repeat buying behavior.

Mobile wallet. An electronic account accessible from a mobile device that stores user payment information such as credit and debit cards. The mobile wallet application enables payment services with the consumer's device.

Show 'n go. This use case occurs when consumers present static images on their mobile phones to the merchant to show proof of purchase, redemption of a coupon, or other related activity that typically involves a manual intervention on the merchant side.

SIM (Subscriber Identification Module). A memory chip deployed in smartphones and tablets. The SIM card can store user identity, location and phone number, network authorization information, personal security keys, personal contact lists, and text messages. Security features include authentication and encryption. The SIM card also can contain other electronic chip applications such as a secure element module to store highly sensitive payment credentials.

Leading the way in mobile payments acceptance are four types of systems: card-swipe hardware with a tablet or card reader attached to the device; mobile contactless; mobile billing, in which charges are billed to the customer's mobile carrier; and text payments, in which the merchant accepts payment through an SMS transfer.

At present, the majority of merchants focus on card-swipe hardware with a tablet or card reader attached to their device and/or mobile contactless. Both of these systems can accept magnetic-stripe and IC chip data, so it is important to distinguish between contact/swipe and contactless.

Contact chip cards provide a better platform for data security and storage than magnetic stripe. Contact chip cards, sometimes dubbed "smart cards," also include a magnetic stripe. Cards that have both the chip and the stripe are referred to as "hybrid" cards.

Contactless/NFC chip technology uses radio-frequency identification (RFID) protocol to process payments. A major difference between contactless and chip-reader POS systems is that contactless does not require a physical electrical connection between the payment instrument and the card reader to exchange data.

In terms of hardware, four readers currently prevail. The first is the dongle, which can be used as a magnetic-stripe reader and plugs into a mobile device (usually a tablet), often using the audio jack. An EMV chip reader, for cards with an IC chip, uses a "chip and PIN" authentication system in which the customer enters a personal identification number ranging from four to six digits. Other EMV cards can be signature-only with a differentiation between the POS (signature) and unattended terminals or ATMs (PIN). The other two are the familiar magnetic-stripe readers and contactless/NFC chip readers.

Options Beyond Payments

Because smartphones are essentially wireless, handheld super computers, the options to conduct commerce are practically limitless—and this is why a merchant must judge how "wired" its customers are. Apps and software, combined with customers' use of social media, can help

Evaluation Criteria for Hardware, Apps, and More

mPOS Device and Data Entry Options

- □ What types of transactions will this product enable me to accept? Credit cards? PIN-based debit transactions?
- □ Am I "future proofing" my business with this device selection?
- □ Will the majority of my customers be able to transact with this device?
- □ Do I need to accept mag stripe cards and EMV chips? Contact and/or NFC?
- □ How secure is this device, and how much risk can I tolerate?
- □ Can my current ISO/acquirer/processor gateway and systems work with this device?
- □ What is the warranty or service commitment from the vendor?
- □ Does the device enable physical security, such as mobile device management?

Mobile Payment Applications

- □ Does the app demonstrate ease of use and compatibility with other apps?
- □ User interface and transaction flow?
- □ How does the register app function with the payment structure? How easy is the register function to use?
- □ Does the app accept the same type of electronic payments that my current system does?
- □ Does the app have the same functions for void, refunds, etc.?
- □ What type of payments does the app accept: mag-stripe, EMV, NFC, and/or contact?
- □ Has the app been tested through a mobile app security testing process?
- □ Can my current ISO/acquirer/processor gateway systems work with this app?

to generate real-time coupons, product reviews, and geolocation based-marketing—customers can receive pop-up coupons on their mobile devices simply as they pass near a store using such technology. On the back end, offerings from vendors can help to streamline operations, including payroll, inventory, staffing, and more.

These kinds of software and apps harness the power of Big Data, previously the province of only the largest of retailers with millions to invest in such technologies. One of the most important decisions that a merchant must make when evaluating the move to mPOS is whether and how the use of Big Data, as part of its operations, can integrate with the payment mechanisms the merchant selects. As such, the selection of an mPOS system can be used as a time to rethink and possibly reinvest in customer relationship tools and back-office operations. These new tools, which can be Cloud-based, can provide real-time information on a merchant's operations.

Risk Management

With new systems come the potential for new risk for merchants. As such, merchants need to address this topic with their product vendors, ISOs, acquirers, and processors. Above all, merchants must be comfortable with the level of risk they are assuming and must balance that risk with the diverse forms of customer payment that the merchants elect to accept—especially in light of the new liability rules governing EMV migration.

With that in mind, here are three types of security solutions that merchants can pursue in relation to mobile payments:

Third-party security providers offer **Point-to-Point Encryption (P2PE)**, which is a combination of secure devices, applications, and processes that encrypt data from the point of interaction (such as a swipe or the reading of an IC chip) until the data reaches the provider's secure decryption environment. Merchants can learn more about

Mobile Payment Complementary Services

□ What complementary services do my customers want? Inventory checks? Online product reviews? Purchase history?

□ What complementary services will support and streamline my business?

□ Integration with my accounting systems? Inventory management?

□ What complementary services will support my sales staff? Work scheduling tools? Instant messaging?

□ Can I capitalize on new analytics with these apps to better understand and serve my customers? Is Big Data applicable for my business?

□ Can these apps help me to "future proof" my business?

10 Steps for Informed Decision Making

1. **Plan, plan,** and then plan some more.
2. **Evaluate your business** and the potential for mobile technology in your business.
3. **Benchmark other businesses** that have made the transition. Keep in mind that people love to give advice.
4. **Review your current and prospective customer base** and estimate their preferences for consumer payments that you'll need to accept.
5. **Review your current payment technology** infrastructure and plan which types of new hardware and applications that you will need to select.
6. **Determine the devices, applications, and infrastructure** and plan which types of new hardware and applications that you will need to select.
7. **Determine the complementary services** that will assist your business and assess their compatibility with your hardware, applications, and infrastructure selections.
8. **Discuss your plans with your ISO**, acquirer, and/or processor, as well as other interested parties (favorite customers, family, tech-savvy friends, etc.).
9. **Contact vendors for competitive bids** on your selections and evaluate at least three scenarios for your mobile payment system.
10. **Plan, test, and launch.** Review your experience and sales data and tweak your strategy and tactics as needed.

this form of solution from the PCI Security Standards Council, which publishes a list of approved providers.

In the **Semi-Integrated Environment**, sensitive payment data is processed in the Cloud instead of on the customer's mobile device. In the case of an mPOS tablet with a cash register application, this solution operates in such a way so that no data is sent through the mPOS tablet other than information indicating that the transaction occurred.

Hosted Card Emulation (HCE) also processes data in the Cloud. HCE allows NFC-based payment applications on the customer's mobile device to communicate directly with a merchant terminal.

For more information on helping merchants make informed decisions about mobile payments, read the full whitepaper "Making Mobile Payments Make Dollars and Sense for Small-to-Medium Businesses" by the ETA Mobile Payments Committee. ETA members can login and download it at http://bit.ly/1BGoDGC. ***TT***

THE BRIDGE CONNECTING YOU TO THE PEOPLE AND PRODUCTS TRANSFORMING COMMERCE.

TRANSACT comes to San Francisco – the hub of global technological innovation – in 2015. And with it comes the world's largest financial institutions, technology companies and retailers. This unique moment in electronic transactions history is the optimal time to join your colleagues and your community. As an ETA member, you save $500 on this can't-miss event. Register today at **transact15.com.**

For *Transaction Trends* readers: Use Code **TT25** to get an additional $25 off your registration.

3.31.15 – 4.2.15

MOSCONE CENTER
SAN FRANCISCO

www.transact15.com

TRANSACT® 15
POWERED BY ETA

CONNECTING THE PAYMENTS TECHNOLOGY WORLD

ETA

Card-Linked in Real Time

Tech experts chart the road ahead for automated digital coupons

Each year, the ETA Strategic Leadership Forum brings payments thought leaders and decision makers together to engage in strategic conversations that profoundly influence the future of our industry. This year at The Breakers in Palm Beach, Florida, the ETA Technology Council convened a closed-door roundtable discussion to address and consider the shift underway in the provision of card-linked offers—digital coupons loaded onto consumers' credit, debit, or store loyalty cards. The conversation not only spurred some fascinating insights, but also resulted in the development of a Card-Linked Working Group to facilitate further consideration of the issues discussed.

In this *Transactions Trends* exclusive, we'll share these experts' insight and expertise on merchant adoption, real-time delivery, and the impact of the growth of mobile payments on the loyalty space.

Participants Included:

Jeff Mankoff, president and founder of vPromos, ETA Technology Committee member, and moderator

Kirk Goldman, senior vice president, marketing and strategy, Toshiba Global Commerce Solutions

Harry Hargens, vice president of business development at Cayan

Phillip Kumnick, head of global acquirer processing, Visa

Adam Spencer, director of merchant sales and acquiring, BBVA Compass

Seamless for Consumers, Valuable for Merchants

All merchants need marketing and loyalty. Loyalty programs offer an opportunity to identify, empower, communicate with, and retain customers. But starting a loyalty program—and sticking with it—can be difficult for a small- to medium-sized business (SMB). Card-linked loyalty programs can serve as an easy way for merchants to start a loyalty program, and an easy way for their customers to participate.

The panelists noted that card-linked programs' ease of use enables shoppers to receive the benefit and reward of couponing in a seamless manner. The rewards and discounts are printed on receipts or in their card statements.

Jeff Mankoff got the panel started by explaining, "While many consumers object to carrying a loyalty card, if enrollment in a card-linked loyalty program is easy, they will enroll. And the automation of the tracking of the loyalty with the credit card makes loyalty participation for the loyalty member and the merchant easy. That means greater loyalty membership and repeat business."

By engaging customers' long-term retention, card-linked offers also maximize, and potentially can expand, the business relationship a merchant has with its customers. Merchants that understand this value should be willing to make the investment, participants said.

"Price is number four on a merchant's concerns [list], whereas a few years ago, it was number one. It's all about getting to know your customer and multiple value adds," said Adam Spencer.

Transformed by Real Time

Efforts to provide consumers with specialized loyalty and reward programs linked to cards have been around for several years, participants noted.

"The greatest challenge with card-linked offers is that they have not been operational in real-time," Mankoff explained. "If they are not in real time, you cannot enroll a customer at the point of sale. We have been seeing great success with enrollment at the POS. And getting the discount in real time, versus cash back, is what consumers expect."

For card-linked offers and rewards to occur in real-time, redemption must take place at the point of sale. Moreover, loyalty and reward programs may seek to utilize card-linked enrollment at the point of sale as well. "Payments technology companies are innovating new and seamless methods of adding shoppers into loyalty programs," Harry Hargens noted. "Easy enrollment at the POS dramatically improves consumer participation. And, these real-time card-linked rewards can give consumers more reasons to eschew cash and checks in favor of paying electronically—a goal that is great for all payments companies."

Panelist brought fresh ideas to the conversation on card-linked implementation, as well as years of insider payments experience. Across the payments ecosystem, the benefit and desirability of loyalty has long been recognized.

"Toshiba has a long history with card-based loyalty programs," Kirk Goldman said. "Many retailers that we work with, particularly grocers, continue to recognize value from the legacy technologies supporting their customized programs. As solutions evolve, the touch points in the store—the point of sale or points of commerce—will continue to play a critical role."

The reliance on the point of sale as a mechanism to facilitate and expand use and provisioning of real-time card-linked offers means that POS companies will emerge as important players and serve an integral role in expanding the card-linked movement.

Effects on Payments

The panelists agreed that the rising popularity of card-linked offers will have a profound impact on the payments landscape. "Companies will have to come into the market and collaborate quickly, or they are going to get left behind. Ultimately, the people who col-

laborate will win," Spencer noted. "To close the loop, acquirers have to have a deal to access customer data so we can drill down the data and find loyalty offers that are relevant to customers."

Hargens addressed strategies for card-linked programs in the ISO channel: "As margins for card processing continue to compress, ISOs and agents need to sell value-added services to survive and prosper. While some big [ISOs] may be able to justify creating their own programs, most organizations will need to partner with third parties that provide these programs."

Ensuring the long-term growth and sustainability of card-linked offers is important to consider. Participants discussed the need to develop industry standards to help convey the upfront costs of automating loyalty and to more effectively bring it to scale for merchants and their customers.

With the changing landscape of the payments ecosystem and the growth of mobile payments, affinity programs have begun—and will continue—to shift to enabling real-time rewards and benefits. Mobile payments such as Apple Pay, Softcard, V.me, MasterPass, and others are changing the game for real-time loyalty benefits. In fact, loyalty programs linked to phone numbers, be it mobile-linked or card-linked, are poised to surpass the previous email-only model.

"Mobile is enabler that brings outside-of-the-store behaviors inside the store," Goldman said. "There hasn't been something yet that changes the customer behavior."

The Future of Card-Linked

Card-linked rewards offer a tech-savvy way for consumers to realize real-time rewards and for merchants to gain loyalty. Technology can limit repeat redemption of offers, while meaningful analytics and data can personalize offers that shoppers really want.

"As SMBs adopt card-linked loyalty, pay-for-performance acquisition tools will empower SMBs to press a button that will deliver offers via Facebook, Twitter, and affiliate networks," said Mankoff. "Consumers will accept these offers and redeem simply by paying the way they normally do—with their credit cards. And the merchant does not just make another sale, but now has a new, card-linked loyalty member."

Given the range of issues discussed, it was clear that there are additional matters to consider as card-linked offers adapt to the changes underway in the payments industry. To facilitate further dialog, the Technology Council launched the ETA Card-Linked Working Group, to be led by Moderator Jeff Mankoff. The working group will examine the landscape of card-linked programs and develop guidance for merchants and acquirers to better understand how the shift to real time is affecting the development and evolution of card-linked programs.

The working group and its insights will raise both merchant and consumer awareness of the benefits of loyalty programs. Leveraging card-linked and real-time technology, upgrading merchants to card and mobile acceptance, and making linked loyalty programs more seamless for all will benefit payments technology companies across the industry. In addition, the formation of the working group will facilitate partnerships and the ongoing collaboration between payments and technology companies in the card-linked space.

ETA will provide updates on the working group's progress in future issues of *Transaction Trends*.

Lori Breitzke

The October 2015 deadline for chip-based POS equipment looms large for merchants. But are they really taking steps to get there—or just talking around the issue? *Transaction Trends* asked Lori Breitzke, president of Atlanta-based E&S Consulting, who is working directly with merchants, acquirers, and issuers to get them up to speed.

How far along is the move to EMV? What are merchants telling you?

Larger retailers have made major progress; small- to medium-sized businesses (SMBs), not so much. A lot of it has to do with confusion on SMB merchants' part. I've been doing webinars for SMB retailers—as well as large retailers and the ISO/acquirer community—since 2012, and I see them on the front lines. They don't understand what EMV means. They don't comprehend that it's not a matter of paying a small penalty each year if they don't upgrade their equipment. They don't see the potential for liability.

It's important to point out that in certain cases, the reluctance is justified. Fraudsters are primarily interested in using stolen numbers to buy expensive items—television sets, computers—that they can resell. Few, if any, are going to use a fraudulent card to pay for dry cleaning, a manicure, food at the supermarket, or a $5 cheeseburger. These merchants know that on some level.

What else is holding things up?

Many merchants ask, "If it ain't broke, why fix it? Why change a system that works? I just want to take credit and debit card payments. I can do it with the equipment I already have." Others aren't sure what's required equipment-wise. I get questions like, "Do I need a PIN pad to accept chip-based payments? Do I need to have a new encrypted key loaded into my system?"

A lot of SMB merchants have misconceptions about the cost of EMV-ready POS equipment. They claim they can't afford it—that's not necessarily true. The monthly charge for hardware that accommodates EMV isn't much higher than the fee for hardware that doesn't.

Training is a roadblock, too. Some issuers are starting to teach consumers about how to use chip cards, but it's mostly being left to merchants…and they have to teach their employees how to help customers complete their transactions the first few times. How many merchants have the time or inclination to do this? How many employees—especially teenagers—will care about getting it right? Not a lot—again, unless there's a merchant incentive.

It also doesn't help that EMV only shores up card-present transaction security. A large number of merchants—from toy retailers to neighborhood restaurants that take orders on their websites—accept payments online. Until we figure out a way to fix the card-not-present side, there's going to be hesitancy.

Which merchant segments are furthest behind schedule? Why?

Besides grocery stores and low-ticket merchants? Petroleum retailers. Retrofitting pumps for EMV is very expensive. Quick-service establishments are slow to upgrade; they have multiple lanes to consider. Any type of SMB merchant that may have very special business software—daycare providers, veterinarians—come to mind as well. That software needs to be updated to work with EMV, and how to do it—they don't have a clue.

When will we see true EMV migration—mass conversion by both large and SMB retailers—and what will it take to make it happen?

I think it will be 2019 at the earliest before we really see this, and it's going to take more than straightening out all of the merchant confusion about what EMV is and what's needed to process chip-based payments.

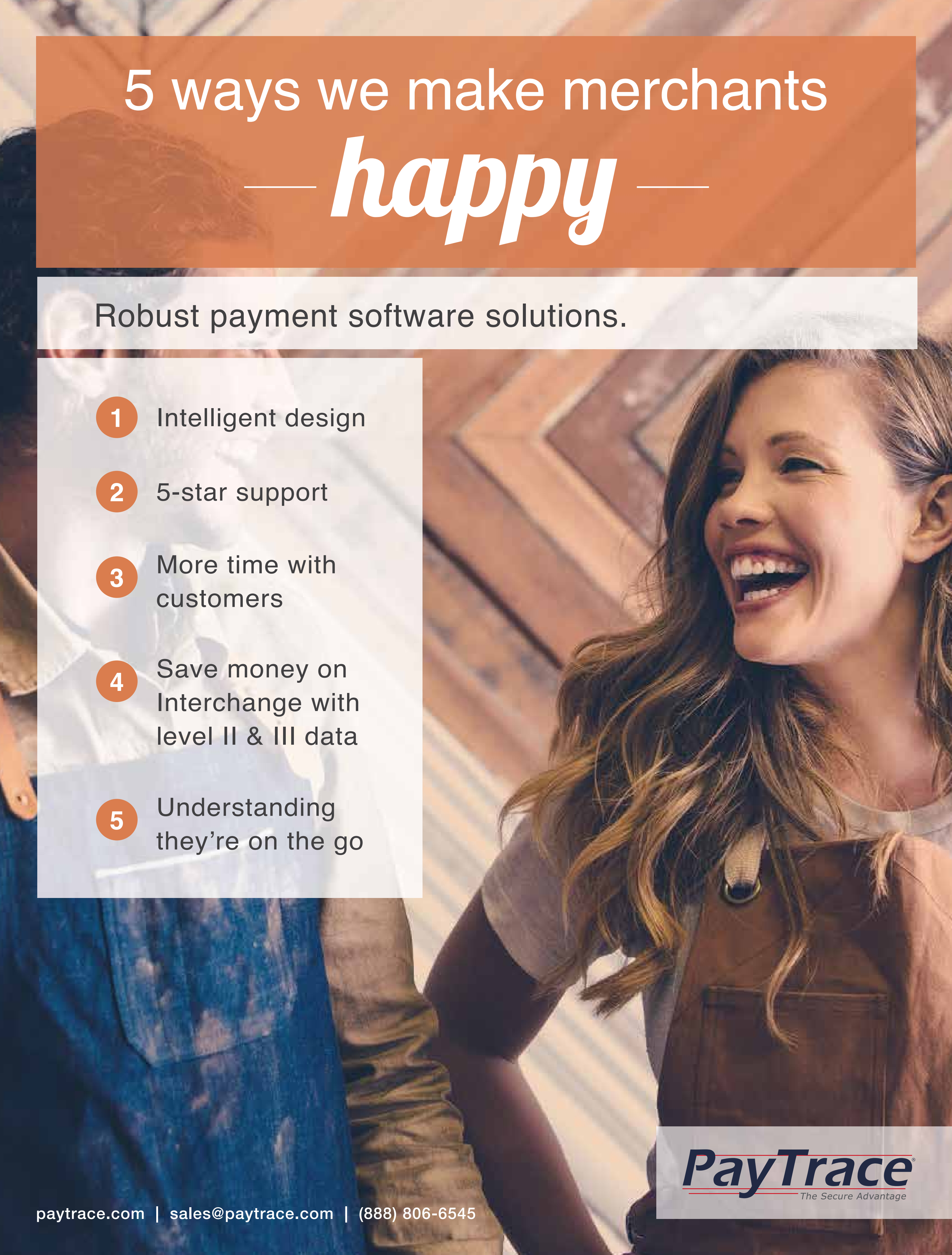
Some of it has to do with the expiration dates on cards. Many banks think the only logical thing to do when it comes to EMV is to wait until consumers' older cards expire before sending new ones with the chip in them. There's a huge, huge pool of consumers out there who have in their wallets cards that aren't going to expire until 2019 or even 2020. If consumers aren't yet carrying chip cards, merchants won't see a reason to switch immediately.

Some kind of merchant incentive is necessary. That's what happened with big retailers. It's silly to think they bought all the EMV devices that were installed in their stores; some came from incentives offered by the card brands. Changes in interchange would be a good incentive. Add an additional basis point—or five—to process transactions, and watch what happens. Quick-service restaurant operators and other low-ticket merchants will think to themselves, "Wow. This is really going to affect the amount of money we can make, and it would definitely be cheaper to bring on EMV."

What can other industry players do to spark migration momentum?

Merchant service providers, ISOs, and value-added resellers need to dispel all the myths surrounding EMV. They need to answer the questions—down to whether, for example, an encrypted key should reload and if a particular piece of hardware is suitable for handling chip-based transactions. And it goes without saying that card brands need to bring incentives to the table. We could spend days looking at all the different factors here. EMV is going to happen—just not at the speed we envisioned. ***TT***

—Julie Ritzer Ross



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

BUY