Exclusive: Read, Learn, and Earn ETA CE Credits PAGE 10

November/December 2015

TRANSACTION trends

ETA
THE OFFICIAL PUBLICATION OF THE
ELECTRONIC TRANSACTIONS ASSOCIATION

Personal Payments

How biometric authentication and wearable devices are evolving

ALSO INSIDE:

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

ACCELERATE BUSINESS | AMPLIFY VOICES | EXPAND KNOWLEDGE

YOUR ETA: NOW

CardFlight has become more profitable thanks to our ETA membership.

As a mobile payments start up, our involvement with ETA, especially TRANSACT, has given us major exposure to the industry and resulted in multiple sales. But ETA membership is more than a single event. It gives us opportunities to interact with clients and business partners in meaningful ways year-round.

Derek Webster, Founder & CEO, CardFlight;
ETA Technology Innovation Awardee

ETA
ELECTRONIC TRANSACTIONS ASSOCIATION
Advancing Payments Technology

ELECTRAN.ORG

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

WHERE PAYMENTS LEADERS CLOSE DEALS

WHERE TECH STARTUPS OPEN DOORS

TRANSACT 16
POWERED BY ETA

4.19.16–4.21.16 | LAS VEGAS
MANDALAY BAY | transact16.com

TRANSACT 16 is the event for payments technology. Produced by the Electronic Transactions Association, the world's largest payments industry trade group. TRANSACT 16 is where you **make connections, secure partners and funding,** and **leverage emerging technologies.** It's the only event where serious business gets done. **Register today at transact16.com.**

CONNECTING THE PAYMENTS TECHNOLOGY WORLD

- Security & Fraud
- Mobile POS Technologies
- Loyalty & Reward
- E-Commerce Payments
- P2P Payments
- App Development
- Retailers
- Digital Currencies
- Financial Institutions

contents

The Official Publication of the Electronic Transactions Association Vol. 20 | No. 6

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
Brandes Elitch, 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

Close Deals and Open Doors at TRANSACT 16

As the year comes to an end, we can confidently say that 2015 was the most innovative year for electronic payments to date, and we expect 2016 to be even better. The payments landscape is now shifting at an unprecedented pace. Capitalize on this momentum by reserving your spot at the only trade show where payments business gets done —TRANSACT 16.

TRANSACT 16 is *the* event for payments technology. It is where you make connections, secure partners and funding, and leverage emerging technologies. You will build influence for your organization, network 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 at TRANSACT 16.

Integration at the POS is a team sport, requiring multiple players and partners to cross the finish line together. At TRANSACT 16, you'll meet more than 4,000 attendees including the ISOs, VARs, ISVs, and tech startups that are driving innovation and responding to consumer demand. ETA knows that TRANSACT 16 attendees will be set the future of payments, because this global event is where the industry has gathered to make history for 25 years.

What's more, for members and readers of *Transaction Trends*, this one-of-a-kind opportunity is even better: You can save 35 percent on your full TRANSACT 16 conference fee if you register before January 15.

I look forward to seeing you in Las Vegas!

Jason Oxman
Chief Executive Officer
Electronic Transactions Association

25 ETA 1990-2015
ELECTRONIC TRANSACTIONS ASSOCIATION
Advancing Payments Technology

Trio of Reports Points to Strong Mobile Payments Growth

The future is bright for mobile payments, according to several recently released reports. Mobile payments—both online at the point of sale (POS)—are expected to gain in popularity over the next few years. Below are some highlights from the latest reports:

Mobile payment awareness has reached a "tipping point" in North America, with 52 percent of consumers aware of mobile payments options, according to Accenture's new report, "2015 North America Consumer Digital Payments Survey." However, only 18 percent currently use their mobile phones to make at least one payment per week.

"Though it's clear that consumers are aware that they can make payments through their phones, continued use of existing payment methods—such as credit cards and cash—and slow retail adoption of modern card readers have caused usage levels to remain stagnant over the last year," says Accenture's Robert Flynn. "This is a clear indicator to banks and retailers that although the digital transformation in payments is progressing, there is still a long way to go before we reach broad market adoption."

High-income consumers and Millennials are the early adopters of mobile payments, according to the Accenture research. Thirty-eight percent of consumers with household incomes of $150,000 or more use their phones to make payments at merchant locations at least weekly, and 23 percent of Millennials do so. The survey also found that Apple Pay is used for more than two thirds of mobile payments in U.S. stores.

Shopping via mobile device is forecasted to grow to a 42 percent share of online commerce by 2019, reaching $218 billion in sales, according to Javelin's recently released "Online Retail Payments Forecast." The growth in e-commerce is attracting online alternative payment providers, such as PayPal Credit, which will displace some traditional payments methods over the next few years. "Consumers are clearly opting for shopping using the smaller screen while on the go," says Michael Moeser, director of payments at Javelin. "Single-click transactions are the holy grail of alternative payments providers, as speed of transaction is one of the top reasons consumers choose an alternative payment option."

The number of Americans who use their phones to purchase goods and services at the POS, via tapping, waving, and similar functionality, is expected to climb steadily, according to eMarketer's "U.S. Proximity Mobile Payment Forecast for 2014-2019." The total value of U.S. mobile payment transactions is predicted to grow 210 percent next year, says eMarketer.

U.S. mobile payments are expected to grow from $8.71 billion in 2015 to $27.05 billion in 2016. The amount of money spent per consumer via mobile is expected to climb from approximately $376 in 2015 to $721 in 2016.

The dramatic rise in mobile payments will be driven by a number of factors, including the fact that mobile wallets (Apple Pay, Android Pay, and Samsung Pay) will become a standard feature on new smartphones, says Bryan Yeager, eMarketer analyst. "Also, more merchants will adopt point-of-sale systems that can accept mobile payments, and incentives like promotions and loyalty programs will be integrated to attract new users," says Yeager.

While approximately 23 million people in the United States are using proximity mobile payments in 2015, a 62 percent increase is expected for 2016, bringing the total to 37.5 million people. Younger consumers are expected to adopt mobile payments at a faster pace than older consumers. In addition, the average price of purchases made via mobile is expected to increase.

Fast Fact

Consumers are spending more on prepaid gift cards this year, reaching an average of **$58.95 spent on physical cards** (up from $57.64 in 2014) and **$56.98 on e-gift cards**, (up from $54.90 in 2014).

Source: "2015 Prepaid Consumer Insights Report," First Data

Contactless Biometric Transactions Begin To Take Hold

The increased rollout of contactless payment services using fingerprint scanners is spurring a rise in the number of biometrically authenticated transactions. Nearly 5 billion such transactions are predicted to take place by 2019, up from 130 million in 2015, according to Juniper Research's new study "Mobile Identity, Authentication, & Tokenization, 2015-2020."

The increase is expected due to a greater availability of fingerprint scanners in midrange smartphones, combined with a growing acceptance of contactless infrastructure at the point of sale. Currently, Apple Pay and Samsung use fingerprint scanners for authentication, with availability limited to the United States, United Kingdom, and South Korea. Both Apple Pay and Samsung are expected to launch in additional markets during 2016, and the convenience of the scanner is likely to make it a primary mechanism for transaction authentication, according to the researchers.

The Juniper report also discusses the importance of security when dealing with biometric data. A breach of biometric data can lead to consumers' online identities becoming irretrievably compromised. In addition, tokenization is becoming an increasingly attractive proposition for acquirers and processors due to the greater prevalence of cybercrime, according to the researchers.

Apple Pay Consumers Seek More Seamless Payment Experience

Since Apple Pay was introduced in October 2014, many consumers have welcomed the mobile payment, but some challenges remain regarding merchant acceptance and overall user experience, according to a consumer marketing report from Phoenix Marketing International.

Within the first four months of its release, the Apple Pay adoption rate rose to 11 percent of all credit card holders (15 percent among smartphone owners). Since then, the adoption rate has climbed to 14 percent. Higher adoption rates are shown among younger consumers: Millennials and Gen Xers currently account for 92 percent of Apple Pay users.

The Phoenix research uncovered several "friction" factors that are reportedly undermining Apple Pay usage growth:

- Nearly half of Apple Pay users have

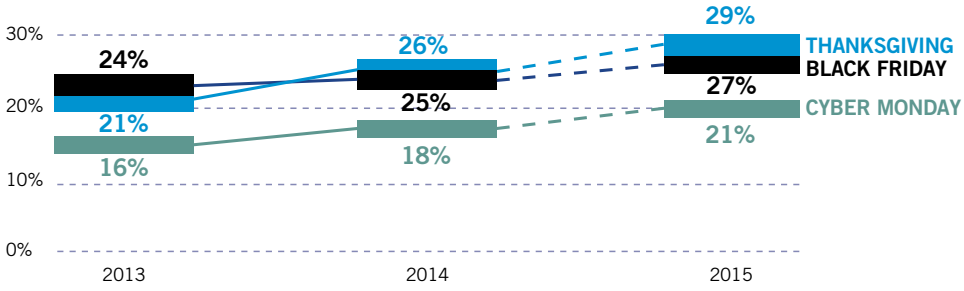
expected Apple Pay to be accepted, only to learn that the specific store they visited did not accept Apple Pay.
- A majority of Apple Pay users continue to encounter problems at the point of sale, including terminals that take too long to use, terminals that don't work properly, and uneducated cashiers.
- There is some confusion regarding customer support; Apple Pay users say they are unsure whom they should contact when there is an error, such as a double charge.

"An influx of inbound inquiries from Millennial and Gen X cardholders creates an opportunity for card issuers to engage customers and differentiate the bank brand," says Greg Weed, director of card research at Phoenix. "Issuers are faced with new challenges to influence wallet position and differentiate benefits and services beyond those that are automatically delivered through the Apple Pay wallet. Future growth still depends on marketers' ability to differentiate the merits of digital versus plastic card transactions."

Infographic

E- and M-Commerce To Reach New Highs During This Holiday Season

Adobe predicts online holiday sales to hit $83 billion, with record percentages of purchases made via mobile device.



Source: "Adobe Digital Index 2015 Shopping Predictions"

ETA continues to be the Voice of Payments into 2016

Year-End Perspectives

By Scott Talbott

As the calendar year and the first legislative session draw to a close, Congress is wrapping up work and heading back to their state or district to begin campaigning for next year's election. At the same time, ETA's government relations efforts continue to have an important impact on your business.

Here's a look back at what has been accomplished during 2015 as well as what lies ahead for 2016.

Congressional Highlights

In 2015, the House and Senate each passed bills to allow the payments industry and other businesses to voluntarily share information about cyber threats with the Department of Homeland Security. The payments industry is at the forefront of preventing cybercrimes. We see data points before they become trends. For these reasons, ETA has long supported these bills, and it was a major focus of our fly-in of ETA executives in September. ETA will continue to push for the bills to allow voluntary sharing of information to become law in 2016.

Congress also will consider a number of bills that create a uniform national standard for companies to follow when notifying customers about a breach. Currently, companies must comply with 47 different state laws to notify their customers in the event of a breach. The payments industry, along with retailers and others, will press for these bills to become law next year.

ETA's continual efforts to educate policy makers are playing out on several other fronts:

- **Patent Reform.** ETA will continue to push for reforms to strengthen the patent system to help defeat "patent trolls." Reforms include making it easier to appeal a patent and introducing procedures to defeat a patent violation claim.
- **EMV.** October 1 marked the start of U.S. migration to more secure EMV technology. ETA has been hard at work educating policymakers about the importance of chip cards, the type of fraud they prevent, as well as more advanced security measures such as tokenization and encryption. ETA's educational efforts and opposition to any technological mandates will continue in 2016.
- **Congressional Payments Technology Caucus.** ETA continues to engage the recently formed Senate Payments Innovation Caucus and the House Congressional Payments Technology Caucus (CPTC). ETA regularly briefs members of the House and Senate Caucuses on the inner workings of the modern payments industry. CPTC recently held its second briefing on the payments industry, where ETA members discussed the intricacies of the modern payment system. The briefing allowed industry experts to inform members of the Caucus on the migration to chip cards.

Regulatory Outlook

ETA expects two actions from the Consumer Financial Protection Bureau (CFPB) next year. First, we anticipate the CFPB, working off of its 870-page proposal to regulate general reloadable prepaid cards, to issue a final ruling. ETA has filed a comment letter expressing our strong concerns with the restrictions proposed by the CFPB.

Second, the CFPB is preparing to issue a proposal to regulate clauses in consumer contracts that require the use of arbitration to settle a dispute. ETA supports the use of arbitration clauses as a quick and efficient way for consumers to address a concern with a financial institution. ETA has met with CFBP staff and will continue to work against restrictions on arbitration clauses.

In addition, the DOL has issued proposed rules to increase the salary level below which employees must be paid overtime. ETA has joined a coalition to express concerns with the proposal, which would weaken the ability of employers to hire or keep the same number of employees.

The DOL also has issued proposed guidance for implementing the Fair Pay and Safe Workplaces Executive Order that would require companies bidding on government contracts to disclose whether there have been any administrative merits, determinations, or judgments against them for labor law violations in the prior three years for. The DOL has defined administrative merits determinations to include unadjudicated complaints and allegations of violations. ETA filed comments objecting to such a broad

definition of administrative merits determinations on the grounds that it may have the unintended consequence of eliminating companies from competition based on mere allegations. ETA also objected to proposed amendments to the Federal Acquisition Regulations that would prohibit government contractors from entering into pre-dispute arbitration agreements with third parties for claims arising under Title VII of the Civil Rights Act or any tort related to or arising out of sexual assault or harassment.

Over the summer, the Federal Communications Commission (FCC) granted the American Bankers Association request for an exemption of the explicit consent requirement of the Telephone Consumer Protection Act for automated calls and texts made to mobile phones by financial institutions to alert their customers to possible fraud, identity theft, or data breaches and to inform money transfer recipients on how to access the money. The ABA filed a Petition for Reconsideration of the FCC's requirement that such calls and texts only be made to the telephone number provided by the customer. ETA filed comments supporting the ABA's Petition arguing that the provided number condition should be replaced by a condition stating that such calls and texts may only be made to customers whose accounts are affected and to money transfer recipients.

State Issues

Washington State's Department of Revenue is considering imposing treating interchange as revenue to payment processors. ETA has been pushing back with the department and state policymakers.

ETA also has noticed a developing trend where state money transmitter departments are attempting to apply their law to the modern payments world, often with troubling results. To help guide state money transmitter departments, ETA held a webinar aimed at educating all 50 state regulators about the intersection of the modern payments world with state money transmitter laws. The event was well attended, and ETA is conducting individual meetings with states. The deck can be found at www.electran.org

The New York Department of Labor has issued proposed regulations on the use of payroll debit cards. ETA filed a letter expressing concern about a number of provisions, including the department's proposal to prohibit a broad range of fees on services that are unrelated to the consumer's access to wages.

Looking ahead to 2016, it is important for payments industry executives to continue to have their voice heard to promote the benefits of quick, reliable, and safe electronic payments. ***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.

BIOMETRICS AND WEARABLES

The New Face of Biometrics

Use cases evolve beyond fingerprint scanning and payments to facial recognition and retail surveillance, loyalty, and more

By Julie Ritzer Ross

ELECTRONIC TRANSACTIONS ASSOCIATION

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/eta-cpp-quiz-biometrics to test your knowledge and earn 2 ETA CPP CE credits per quiz!

Bonus Audio Content: Log in to listen to "Authentication Methods To Expand the Future of Payments" from TRANSACT 15. Visit http://bit.ly/1IryZV7.

Biometrics has long been the stuff of science fiction and Hollywood. Over the past few years, however, these futuristic scenarios have become a reality, with the use of biometric technologies such as fingerprint scanning and facial recognition becoming increasingly commonplace.

A look at market growth confirms the trend: According to Biometrics Research Group Inc., the market for biometric systems—including fingerprint, face, iris, palm, voice, and vein recognition, and more—will grow to $15 billion in 2015. The firm predicts that automated fingerprint identification systems and fingerprint biometric technologies alone will account for two thirds of that market share, or $10 billion.

Moreover, "a significant portion of market activity is revolving around, and will continue to revolve around, payments," says Chris Bucolo, senior manager, 403 Labs, a subsidiary of accounting, advisory, investment banking, technology, and managed services firm Sikich LLP. New use cases are coming to the forefront as new payment modalities emerge, and merchants' interest in biometric solutions for loss prevention and customer engagement is spurring adoption for retail use beyond payments.

Identification and Verification

On the payments side, mobile and e-commerce are a firmly entrenched use case for biometrics. "The global explosion of mobile payments, in particular, will drive the need to have a more secure authentication system, and an alternative to traditional authentication will be Cloud-based mobile biometrics" of one type or another, says Bob Graham, senior vice president at Virtusa, which provides IT consulting, systems implementation, and application outsourcing services. Although Apple created momentum for fingerprint-based authentication with Apple Pay, Graham points out that the roster of applications transcends mobile wallets. Case in point: Over the past few months, mobile banking and credit card apps, such as those offered by Bank of America and American Express, have started to use fingerprint-based technology. Customers and cardholders now have the option of using a finger scan instead of a password to access their accounts on their smartphones.

For transaction execution, PayPal and Samsung have partnered to allow PayPal transactions initiated on Samsung Galaxy S5, Tab S, Note 4, or Alpha smartphones to be completed with a finger scan rather than a credit or debit card. PayPal merchants are sweetening the consumer incentive with deals and discounts accessible only from Samsung fingerprint-enabled devices.

Fingerprints are and always will be considered a solid form of identification "because they are captured and stored on the mobile device and not online or on a network," asserts Dave Rockvam, vice president of product management, Entrust Datacard. "The only way to fool this kind of identification is to physically lift someone's print, but mobile operating systems are new and advanced enough to prevent malware from lifting fingerprint key information."

Credit card networks also are getting in on the act. In September, Visa announced a new specification that will integrate fingerprint-based authentication with Europay, MasterCard, and Visa (EMV) chip card transactions. The specification is structured for maximum security—fingerprints may be scanned and encrypted before being validated, and biometric data may be validated directly on the EMV chip card rather than transmitted to another server and database. (Issuers do, however, have the option of authentication using their own secure systems for transactions executed within their own environments—such as on their ATMs.)

A pilot-test of the specification with Absa Bank in South Africa is now underway. Visa reportedly aims to submit the specification to EMVCo, the global regulatory body that manages all EMV specifications, if the trial is successful.

Not surprisingly, both MasterCard and Visa have additional plans for biometric-based payments. Visa has devised a technical blueprint for consumers to verify their identity during in-store transactions through finger scanning, and possibly by presenting a palm or face, according to a spokesperson. MasterCard is looking at ways to incorporate voice recognition and other biometric technologies, such as heart rate measurements, for cardholder authentication.

The latter has already been done in Canada, where Nymi has kicked off several pilot programs using its

Nymi Band wrist-worn heart monitor. Payments are initiated by tapping a sensor on the band against an NFC terminal; wearers' measured heart rate provides the authentication. Shawn Chance, vice president of marketing, expects additional traction for the Nymi Band as multi factor payment authentication becomes the norm.

Facial Profiling

Perhaps the most cutting-edge application of biometrics in online and mobile transactions centers on facial recognition technology. In an August report, Transparency Market Research forecasted the global market for facial recognition technology to reach $2.67 billion by 2022, up from $1.307 billion in 2014.

This fall, MasterCard launched two separate pilot programs—one in the United States and one in the Netherlands—that ran through the end of October. At press time, the card network had just announced that it would expand the program to bricks-and-mortar stores and e-commerce services in the United States beginning in mid-2016, and in the rest of the world in 2017. The U.S. pilot involved more than 200 First Tech Credit Union employee participants who used a smartphone app to make mock virtual transactions via either facial recognition or fingerprint biometrics. In the Netherlands, the initial trial was conducted in conjunction with International Card Services (ICS) and involved 750 ABN Amro cardholders.

Here's how the "Selfie Pay" trial worked: First, participants downloaded MasterCard's Identity Check app and transmitted a selfie to the card network for storage in its servers. If the merchant required that users' identity be verified before purchase, participants received a push notification on their mobile device that opened the app. Once the app was open, cardholders held up their smartphone and blinked, taking a selfie. (The blinking step ensures that the real cardholder, and not someone using the cardholder's photograph, is making payment.) Then, a facial recognition scan within the app converted it to a series of ones and zeroes. If the numbers matched the initial image captured in the app, the payment was authorized.

While combating credit card fraud was MasterCard's primary intent in introducing Identity Check/Selfie Pay, it also is expected to help improve the online shopping experience by eliminating problems caused by forgotten passwords, Ajay Bhalla, president, enterprise security systems, said in a statement when the initial pilot was announced. According to a recent MasterCard Global Consumer Survey, 53 percent of shoppers forget crucial passwords more than once a week and lose more than 10 minutes when resetting them. More than one third of consumers consequently abandon an online shopping cart, and six in 10 claim forgotten passwords have led to missing out on time-sensitive purchases, such as for concert tickets.

A Marriage of Technologies

Although facial recognition has gained traction in the payments space on its own, some recent applications make the technology a component of a larger solution—for example, one whose primary purpose is to thwart account takeover and facilitate secure authentication for high-value and/or high-risk transactions. Such is the case with Perceive, rolled out in September by Socure, a provider of real-time online identity verification solutions. Perceive has at its base the vendor's Socure Social Biometrics platform, which analyzes user activity on social media, mobile apps, and other online sources to identify behavioral patterns. A proprietary "entity resolution system" compares the face of each individual accessing an account or making a transaction with information from the platform, confirming or denying that the person is who he or she claims to be and immediately delivering an authenticity rating to the requesting financial institution. Other proprietary technology within the system allows facial features to be recognized with the front-facing

What's the Word?

The biometrics market has a vocabulary all its own. In fact, the term "biometric" can describe both a biological and behavioral *characteristic* and the *process* of recognizing an individual based on that characteristic, according to the National Science and Technology Council Subcommittee on Biometrics and Identity Management. Here are a few common words with particular meanings that every payments professional should know:

Enrollment. *First basic function of biometric systems.* The process of collecting biometric sample from an end user, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.

Extraction. The process of converting a captured biometric sample into biometric data that can be compared to a reference.

Feature. Distinctive mathematical characteristic(s) derived from a biometric sample; used to generate a reference.

Identification. *Second basic function of biometric systems.* The biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric sample is compared to all of the references in the database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification (sometimes called a "watchlist"), the person is not guaranteed to be in the database.

Model. A representation used to characterize an individual. Behavioral-based biometric systems, because of the inherently dynamic characteristics, use models rather than static templates.

Reference. Biometric data stored for an individual for use in future recognition. A reference can be one or more templates, models, or raw images.

Template. A digital representation of an individual's distinctive characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison.

Verification. *Third basic function of biometric systems.* A task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.

Sources: "Biometrics Glossary," The National Science and Technology Council Subcommittee on Biometrics and Identity Management; "Biometrics 101," International Biometrics and Identification Association

camera found on standard smartphones. It also checks to ensure that the system is not being "spoofed" by a photograph or video animation instead of a real face.

Sunil Madhu, Socure's CEO, claims a combination of facial recognition and social biometrics comprises a better option than device fingerprinting, click-flow, and other forms of user behavior analysis, and also is a better option than "out-of-band" authentication via SMS or email, which involves multiple steps. Confirming identity through remote facial biometrics also eliminates the need for passwords, which remain the primary point of vulnerability for account-takeover fraud, Madhu adds.

Moreover, social biometrics has been incorporated into Fraud Prevention That Learns, a software solution from data science company Feedzai, to create a "plug-and-play" system that marries online- and social data-based authentication with fraud-risk scoring. The system assesses clickstream, access frequency, and the presence of malware signatures, among other methods, to determine that risk. In addition to transaction authorization, use cases for the combined system include merchant signup (verifying, underwriting, and monitoring merchants against collusion and insolvency), account opening (onboarding and verifying new account and "thin file" applications), chargeback management (prevention of payment chargeback reversals, disputes, penalty fees, and merchandise loss from fraudulent sales), information services (advanced data visualization), and loss prevention (monitoring of internal processes and external data sources to guard against data exfiltration and employee collusion).

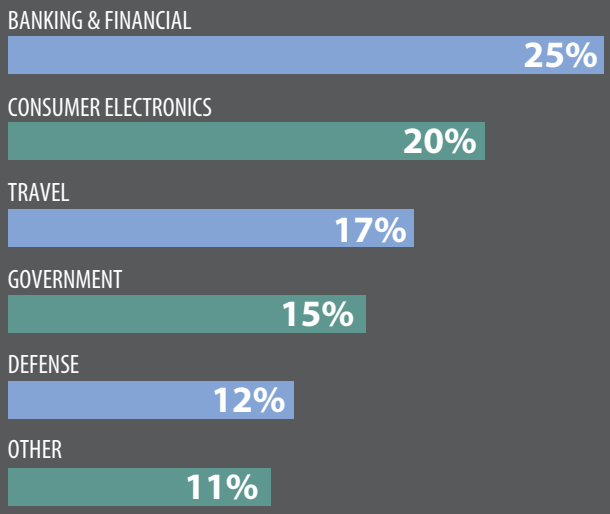
Retail Solutions

The roster of use cases for biometrics also has expanded to broader retail solutions. For instance, merchants have started to add facial recognition technology to their arsenal of loss prevention solutions, employing it to keep tabs on shoplifters. Target is reportedly using facial recognition, and FaceFirst, a software provider, claims a number of large retailers have deployed its facial recognition solution specifically designed for stores.

Merchants' loss prevention teams, a FaceFirst spokesperson explains, can take digital photographs of previously caught shoplifters and load them into a database. (Laws prevent photographs from being taken without criminals' permission, but most will accede to the capture and storage of their facial image and agree not to return to the store if the retailer agrees to drop or not press charges, the spokesperson says.) When an individual whose photograph resides in the database enters the store, a manager or loss prevention staff member receives an email, text, or SMS alert. The retail version of FaceFirst also has the capability to download "watch lists" from other agencies, such as local police departments, and to be used on smartphones as well as at fixed locations. Employees can photograph suspects with a smartphone camera and conduct a check to determine if the individual's information is in the system, if he or she somehow evaded the main camera at the store's front entrance.

Biometric Market Share

Last year, the "global biometric applications market was approximately $10 billion," according to FindBiometrics. Banking, finance, consumer electronics, and travel comprise more than half of the market share. Here's a breakdown of the numbers:



Source: "The Global Biometric Market" infographic, FindBiometrics in partnership with TechSci Research

NEC Enterprise Biometrics has unveiled a similar retail-focused system called NeoFace Watch. While the company would not identify users, several merchants are said to be using it for geofencing VIP customers, greeting them, and providing an enhanced level of service or special deals.

The company also developed a retail digital signage solution with Microsoft, called Inception, which uses a combination of face recognition technology with other in-store solutions to promote customer engagement. NEC's facial recognition technology detects shoppers' age and gender while Microsoft's Kinect sensor identifies their proximity to and/or interaction with a particular display or group of products. Different distances, interactions, and shopper attributes then trigger different digital signage content, such as static or video advertisement screens, product pricing, technical specifications, user reviews from the web, special offers, and more. In addition to bolstering customer engagement, the solution is intended to give merchants a better understanding of which customers are buying which products, by age, gender, and time of day.

Biometrics and biometric use cases have clearly evolved, particularly within the past few months, with more modalities on the way. For example, palm vein biometrics is showing promise in certain mobile payment applications, according to Scott Hess, vice president, consulting, user experience and innovation, Fiserv. However, sources agree that the market is still in its infancy, with myriad twists and turns yet to come. ***TT***

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

Ready To Wear

By Ed McKinley

There are a lot of wearable payment devices out there, but watches and wristbands may have the most staying power

Payments vehicles are no longer confined to the pocket or purse. With the advent of wearable computing devices, tech-minded consumers are beginning to immerse themselves in transactions that originate from their eyewear, smartwatches, not-so-smart watches, wristbands, rings, gloves, cameras, key chains, clips, shoes, clothing, and even tattoos.

But wearables remain in their infancy, and not every form factor seems likely to reach maturity—let alone survive to a ripe old age. The devices worn on the wrist seem most likely to find an audience, according to a consumer survey and interviews with pundits who contemplate the future of technology.

"More people will have some sort of smart device on their wrist in the next few years," says Todd Ablowitz, president of Double Diamond Group LLC, a payments consulting company. "Look at smartphone adoption, and it may track a similar pace."

One out of every three smartphone owners has already acquired a wearable, usually one that is worn on the wrist, according to a study released early this year by Stratos Bluetooth Connected Card, which makes aggregated cards. Among those surveyed who have wearables, 53 percent are wearing smart wristbands, and 24 percent are brandishing smartwatches.

Using smartwatches to make payments simply makes sense because the devices are set to proliferate, according to Ablowitz, who plans to purchase one for his daughter's birthday—which he says demonstrates how widespread smartwatches seem likely to become. "I would never get an 8-year-old a phone in a million years," he notes.

Still, the tipping point for smartwatches doesn't appear imminent. "Sure, a payments geek like me is going to use my Apple Watch everywhere I can," says Ablowitz. "I've used it at McDonald's. I've used it to get on planes. I've used it at Whole Foods. But it's going to take a while before you see people doing it all over the place."

And smartwatches have their downside, cautions Yaniv Chechik, manager of product development for Zooz, an Israel-based payments platform that aims to handle all of a retailer's payments needs. "I sat down for a conversation with this very, very smart software architect, and he kept looking at his watch every 10 seconds," Chechik complains. Smartwatches may speed up a purchase at Starbucks, but they're taking a toll on human interaction, he says.

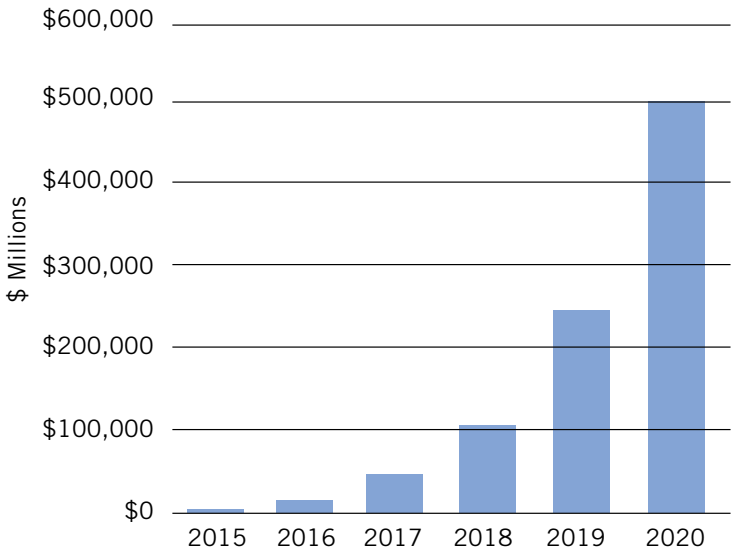
Wristband fitness activity trackers also are worn on the wrist and able to make payments—but less likely to wreak havoc upon verbal exchanges. These devices are available from such companies as Jawbone, Fitbit, Microsoft, Garmin, Samsung, Nike, and others.

"It's all about convenience, and what's more convenient than to have payment capability right on your wrist?" says Mimi Huggins, public relations manager for Jawbone. Fitness trackers seem especially handy when it's time to make a payment because many wearers seldom take them off—even to shower or sleep. Truly dedicated users often choose to keep the devices on their wrists 24/7 so they can keep tabs on their heart rate at rest or while they're sleeping, as well as when they're working out, she says.

More casual athletes who wear a wristband only when

Wearable Payment Transaction Volume

World Markets: 2015-2020



Source: "Wearable Payments," Tractica

they're exercising still find the devices are there to buy a Gatorade at the gym or a cup of coffee in the middle of a jog—times when they prefer not to burden themselves with cash or cards. "Those devices will have a payment capability as NFC readers become more ubiquitous," Ablowitz says.

Jawbone, for example, is taking wristband payments seriously, according to Huggins. The company has replaced its original four-year-old wristband with a new line that includes a model that initiates transactions, she says. It's now offering the basic UP2 for $99, the upgraded UP3 for $179, and the UP4—which is really the UP3 with payment capability—for $199. A pod-like basic model retails for $49.

The company announced all three wristbands in April and began selling them on its website in July. Best Buy and Amazon offer the UP4 online, and all three are scheduled to appear soon in bricks-and-mortar stores.

"There's a little NFC chip in the strap of the device," Huggins says. "You physically tap on a contactless payment terminal where American Express is accepted. You hear a beep that indicates the tap was complete, and you're done."

The company is working only with Amex. "They've been a great partner, but down the road we'll be exploring other partnerships," says Huggins.

Jawbone chose Amex because of the card issuer's devotion to security, Huggins adds. The system substitutes a token for the credit card information so the wristband never carries sensitive data. A user who loses a tracker can go into the app and disconnect the card without being near the wristband. "We wanted to make it as secure as possible."

But the public needn't worry too much about security with wristbands or smartwatches, Ablowitz says. "You use your phone all the time so you would realize if you lost it," he says. "You always have your wristband on."

Besides, devices are becoming less vulnerable to data thieves as the industry continues to combat fraud. "So many security measures are being implemented these days, that if the system is set up safely I don't see that as being any kind of problem," Ablowitz says of security concerns.

Meanwhile, more retailers are preparing their stores to accept NFC payments from devices like wristbands. Jawbone payments, for example, are now accepted at Whole Foods Market, Trader Joe's, Walgreens, and in taxis, and the list continues to grow.

While acknowledging the convenience of using a wristband to pay at the gym or on the jogging trail without carrying cash or cards, Chechik still considers the wrist-borne wearables market limited. "It's a winner, but it's a niche," he says. "I don't see people going into The Gap and buying a pair of jeans with a wristband."

The market is failing to grow prodigiously because consumers are clinging to the habit of using plastic cards, Chechik asserts. He describes standing in a sales line in California and watching consumers in action: "I saw the coolest people," he says. "They were wearing their smartwatches but still reached into the wallet and used the credit card."

Early adopters seem quick to take up the latest technical wizardry, but most consumers seem content to stick to the old ways for a long time. It's up to the payments industry to help them form new habits, Chechik says.

What's more, wearables sometimes don't function as well as they might, Chechik lamented. In a spinning class in Israel, he was wearing a cycling glove with a chip that connected to his gym account. The account, in turn, connected to a credit card. A problem arose when he was standing near a soda machine in the gym and bent over to tie his shoe. For some reason, a soft drink spontaneously rolled out of the vending machine and seemingly charged itself to him, he says.

Even without such malfunctions, problems can crop up with wearables because of human oversights. If a woman wears her boyfriend's jacket and it's been imprinted with a QR code that makes payments, for example, she could charge merchandise to his card, Chechik says. If a parent

with a key ring that makes NFC payments lends a car to a teenager, the teenager could initiate a spending spree.

Off the Cuff

Smart eyewear, on the other hand, could make payments without so many human liabilities because people seldom share their glasses with others. At the same time, the glasses could supply information to help consumers make purchasing decisions. Google Glass has garnered most of the attention in this category, but Hololens by Microsoft and a host of other smartglasses are either available or in development. Could they be a more viable consumer option?

Not likely, says Ablowitz. Smartglasses will prove useful in such fields as surgery, aviation, or high-tech construction, but they don't have much of a future in payments. The trouble began when Google introduced its entry as more of a science project than a consumer product, he says. But perhaps that feeble marketing attempt doesn't matter much: Consumers aren't about to walk around making payments with their eyeglasses, he asserts.

Whether the masses take to smart eyewear in great numbers or not, other types of wearables have varying chances of success. Clips that attach to clothing could be a practical solution because of the many ways consumers can use them. Shoes, however, might seem an odd place for a computer chip. Payment tattoos could strike many as an example of taking consumer culture too far, and watches that make payments but have few other computing capabilities might not find a clientele.

Heavy hitters among financial institutions will probably continue to test wearable devices as payments vehicles, say experts. Examples include the payments wristbands explored by U.S. Bank, the payments-capable rings tested at MasterCard, and the payments glove pioneered by Barclaycard.

In the meantime, consumers continue to follow their own inclinations, and they're indicating some interest. Among the smartphone owners quizzed in the Stratos Card survey, 75 percent say they plan to buy a wearable. Although wristbands and smartwatches accounted for most of the planned purchases, other form factors also attracted consumer interest. Some 29 percent say they might buy a wearable camera, while 19 percent would consider smartglasses. Less than 10 percent say they might buy smart clips, smart shoes, or smart clothing.

While 48 percent say they would use their wearables more if they could make payments, not everyone with an interest in wearables intends to use them for payments, the survey also showed. Less than half (43 percent) say they would like to make payments in stores with their wearable devices.

Still, enough consumers have at least dabbled in transactions via wearables for research firm Tractica to predict wearable payments will drive more than $500 billion in annual transaction volume by 2020. ***TT***

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

Diagnosis: MEDICAL

By Ed McKinley

From partnerships with ISVs to prospecting and research, what ISOs need to know to break into the health-care vertical

Providing transaction services in the health-care field isn't for the faint of heart. But ISOs who persevere, do their homework, and find a niche can earn great margins, enjoy outstanding retention, and benefit from copious referrals, say experts.

"There are certainly easier industries to get into," says Chris Lee, president of North American strategic partnerships and emerging markets for Moneris Solutions. "But as health care attempts to go more electronic, it's been a great vertical."

The first task in entering the market is to sort through the $2.9 trillion industry for a suitable specialty. Obvious possibilities are the offices of doctors, dentists, orthodontists, psychiatrists, chiropractors, optometrists, and more. Bigger medical enterprises include clinics and hospitals. Cosmetic surgeons, whose large-ticket services aren't covered by insurance, require hefty payments from patients.

Additional possibilities, however, may not come to mind so readily, says Mary Winingham, founder of MirrorConsulting. Labs that aren't affiliated with hospitals are becoming a force in health care, she says. Consumer demand is driving these independent businesses to offer medical services ranging from DNA testing to colonoscopies and mammograms. Insurance companies usually don't cover tests conducted without a doctor's order, so patients' payments increase.

"I could drive into Milwaukee and get an MRI for $600," says Winingham. "I don't have to have an order from my doctor or anything like that."

Opportunities in health care for patients that aren't human also exist. Veterinarians represent a $14.4 billion annual business where insurance doesn't play a large role, and pet owners' payments are mostly out of pocket.

Early Observation

Whatever medical payments specialty an ISO chooses, it's vital to become a consultant and not just a transaction services salesperson, advises Afshin Yazdian, president of core acquiring at Priority Payment Systems, a large ISO that specializes in health-care payments and other verticals. "Medical practices are looking for a solution that includes payment processing, but encompasses other aspects of managing their practice," he says. "It is critical for sales agents to understand these needs."

Because medical payments constitute a niche, learning the specialized language of the clientele and the inner workings of their trade is vital to success, Winingham says. A working knowledge of a medical specialty can require walking the aisles and networking at trade shows, poring over trade journals, and frequenting the websites of trade associations. It helps if the ISO starts with a natural interest in the particular type of medical practice, Winingham adds.

Early in the research process, it's also wise that ISOs ensure the niche can provide enough volume to sustain the business model. "If you have to feed 100 sales guys, you'd better be sure there's enough in that niche market," Winingham cautions. "If it's just you and two other guys going after it, the numbers don't have to be so great."

After settling on a sector, find a friend in that market to help navigate the first couple of deals. Strike up a relationship with the family dentist, for example, and get to know the business and the players. Having an ally helps prepare an ISO for the first pitch in a new specialty, Winingham says. Without previous exchanges with an inside confidante, a sales call can fall flat. "If they ask if you're integrated with Turner [a medical equipment, planning, and management company], and you don't have a frame of reference for that question, you've got a problem."

In the search for prospects, Winingham advises contacting the state department of commerce and perhaps the state health department for lists of licensed practitioners in the chosen specialty. The lists cost little or nothing, and the state makes sure they're up-to-date. "It's typically in an Excel spreadsheet, and you can sort it by Zip code and see if you have two or 200 in the footprint where your team is selling," she says.

Good research also should help uncover specific prob-

Acute Need for Trusted Security Advisors

Something is often missing from the software that health-care providers use to run their businesses. ISOs can obviously add the payments function, but their consulting-style services also should help bolster system security.

"After we find a software partner, then our relationship management group consults with them on what their requirements are," says Chris Lee, president of North American strategic partnerships and emerging markets for Moneris Solutions. "In the case of card-not-present, we might be providing end-to-end encryption, tokenization, and security features to protect the data."

As with any kind of business, security in the health-care field requires guarding against criminals bent upon infiltrating databases to steal card data and identity information. But with medical practitioners, security includes helping clients with signature capture that's required to comply with the Health Insurance Portability and Accountability Act of 1996, better known as HIPAA. "We make sure there is a device to capture the signature—or connect their software to our host for processing," Lee says.

These days, the security consulting function for ISOs concentrating on health care also includes teaching the independent software vendors and the health-care practitioners about the shift to Europay, MasterCard, and Visa (EMV), Lee says. To that end, Moneris has produced web seminars on EMV for partners and customers.

Being that trusted security advisor is an essential element to working in the health-care niche, because the other vendors that focus there can feel out of their element when dealing with EMV and security, Lee observes. That unfamiliarity can leave health-care software companies vulnerable to shady operators. "Do they need it or not?" she says of EMV. "You had people walking in the door and saying their terminals aren't going to work in October—all that craziness."

lems, such as a weakness in reconciliation, for example. That sort of information can help mold a solid business plan. "Your research should lead down a pretty specific path," she says.

But research also takes time. After a year of study, ISOs typically find themselves ready to begin knocking on doors to make sales calls, according to Winingham. Even then, they may look back at the startup period and see plenty they would now do differently. "People underestimate how long it will take to become an expert in the market," she adds.

Initial Treatment

Even with the best preparation, an ISO should build a medical specialization business gradually, observers agree. It won't work to begin by trying to get in the door at someplace like Community Health Systems, with its 30,000 beds in 198 hospitals in 29 states.

Instead, start small. Describing a realistic approach, Winingham says that "you start, you stumble, and you go forward. Then you might change your strategy a little bit and go forward again."

Winingham conceptualizes the medical payments specialty business as three tiers, and she advises ISOs to begin with the lowest level, which she calls "the standard one-off." Those include the typical offices with one or two doctors, dentists, or chiropractors. Tier I practitioners typically have some software, but ISOs may have an opportunity to place a countertop or virtual terminal there.

Tier II could include an office with six dentists and 12

technicians, Winingham says. That level can require payments be integrated into a practice management software system that electronically juggles a practitioner's appointments, inventory, personnel, insurance adjudication, and other business operations. "Find out who the software vendors are," in a particular niche, she says. "Go to them and find out what it would take to integrate or how you can work side-by-side with them."

The increased complexity of integration brings significantly larger opportunities. Forming relationships with independent software vendors (ISVs) and other suppliers in Tier II can bring ISOs referrals for transaction business. One company that has taken advantage of those referrals is Moneris. "Our approach has been to partner with software providers and medical billing companies in the health-care space," says Lee.

For example, Moneris works with Henry Schein Inc., a large publicly traded company that distributes products and services to doctors, dentists, and veterinarians. The relationship opens the door to all of those fields. Moneris does not send salespeople out to seek medical accounts. Instead, they work exclusively on closing deals that begin as referrals, she says.

The benefits of such relationships accrue for both parties. Moneris' technology can help some its partners by providing encryption and other security features, says Lee. When integrating with another company's software, Moneris exercises caution to avoid disruption.

Working that closely with an ISV also requires coordinating customer service. "If we find out on our customer service desk about a problem with software at the XYZ company, we make sure to notify the appropriate folks at their site and vice versa," Lee continues. As part of the bargain, ISOs also may find themselves advising their partner companies on the ways of the payments world. That's been especially important lately with the advent of Europay, MasterCard, and Visa (EMV), she says.

Tier III, the level for hospitals and other larger entities, carries the longest sales cycles and demands the greatest knowledge of the industry, according to Winingham, but that doesn't necessarily preclude ISOs from doing business there.

Many hospitals, even a smallish 100-bed facility, operate as a bundle of fiefdoms with separate business operations and computer systems for the pharmacy, emergency room, gift shop, ambulance service, and other departments. "There is not the level of consolidation that you would think there is," she says.

That means more than one payment processor could land contracts in the same institution. "We might do processing just for the cafeteria or break room," Lee says. The work requires a team of developers who work on certifications so that software can connect with Moneris for processing. Counting salespeople, tech support, and relationship managers, about 20 of the company's employees focus on medical payments. "We're doing certifications every day for our partners," she adds.

The fragmentation lends complexity and problems, but it also fosters opportunity. At a single hospital, ISOs should not be surprised to find themselves talking to a chief financial officer, the information technology staff, a procurement group, and other business centers, says Winingham. "I would not recommend starting there," she says of hospitals, "but that's the holy grail and where you could end up."

Critical Care

Health-care providers are among the last in the United States to receive a high number of checks, especially if they're invoicing patients. So it's important for ISOs to expand beyond card transaction services and promote remote deposit capture services (RDC). Failing to do so can be a deal-killer for ISOs attempting to operate in medical payments.

Suppose a medical account accepts credit cards for 60 percent of its transactions, says Tom Cunningham, director of marketing and strategic partnerships for iStream Financial Services, which offers automated clearing house (ACH) and a niche transaction processing platform as well as RDC. "I can get you the other 40 percent that comes in as checks." Switching from cards to checks also greatly reduces the fees involved in accepting payments, he says.

What's more, millions of Americans don't have credit cards or bank accounts. For those who receive government benefits, iStream facilitates electronic access, which could help improve collections in the medical field, Cunningham says. "Health-care entities on average collect 43 cents of every dollar after seven collection attempts. That's pathetic."

Bringing in systems that help medical providers collect copays at the point of sale in their offices also could improve cash flow, according to Cunningham. Not a single patient will volunteer to cough up a copay, he says.

Still, the payments industry isn't clamoring to get into the medical niche. At a recent gigantic medical conference that Winingham attended, only a few payments companies, such as TransFirst, Bluefin, Vantiv, and First Data, were there, she says. What's more, some of those companies were seeking only the "whales" of health care and would not pose a threat to ISOs.

And by all accounts, it takes a lot of work to break into the vertical and remain relevant there. But an ISO occasionally can wind up there with minimal effort. When an ISO boasted to Winingham that he specialized in medical payments, she asked how many of his accounts were medical and how many weren't. He replied that 10 of his 5,000 merchants were in health care. "Unless those 10 are big," she says, "that's not a niche. That's a coincidence." ***TT***

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

Identifying the Risks in Mobile Payments

As fraudsters ramp up efforts to steal data, merchants must be educated

By Brandes Elitch

Merchants have enough to do just managing their brand, without giving a second thought to how payments happen. They take security, speed, and reliability for granted. Large retailers want to close the gaps between mobile, online, and in-store payments to support commerce across all of their consumer touchpoints. They know they can gain from having a digital presence, and they know their current POS systems are holding them back from providing a seamless consumer experience.

These merchants don't have the motivation, the interest, or the bandwidth to get involved in what, to them, is an increasingly complex netherworld of payments: hardware; software; the Europay, MasterCard, and Visa (EMV) standard; near-field communication (NFC); tokenization and encryption; PCI compliance; mobile wallets; mobile devices; and operating systems. Even for independent sales organization/merchant service provider (ISO/MSP) salespeople, the payment environment has become almost too complex.

But merchants do understand the concept of risk in mobile payments. IBM and the Ponemon Institute recently reported that the average cost of a data breach is $3.79 million, and the cost of each lost or stolen record is $154. Given such data, merchants will want their ISO/MSP to explain the concept of risk and strategies for managing it.

Trends in Mobile Payments

Most payments still take place at the POS. NFC, brought back to life by Apple Pay, allows payments from a smartphone or a wearable device at the POS, if the merchant has an NFC-capable terminal. Android and Samsung offer a similar solution but without the need for NFC.

Conversely, a mobile device can function as the POS terminal or cash register, or—more accurately—a mobile process. An app captures the card data via a swipe—for example, via Square. PayPal and Amazon both offer a proprietary mobile platform. All of your credentials are stored there, and the buying process is simplified since there is just one account with the platform provider.

Alternatively, there are closed-loop payment products (such as a single merchant wallet) or open-loop payments (such as Google Wallet or Apple Pay). Most of these use NFC, a bar code, or a QR code.

Finally, there is the option to have the telephone carrier handle the billing, known as "direct carrier billing." Here, the merchant is paid by its wireless provider; this is not a service that an ISO is likely to be reselling.

Four years ago, Google introduced its mobile wallet. The consumer could wave or tap a handset instead of swiping a piece of plastic. Since then, consumers have hesitated to adopt mobile wallets and NFC, and merchants have not seen any real consumer demand. ISOs have not convinced merchants that there is any incremental value to mobile payments, unless they can show that it is cheaper, which remains to be seen.

Small merchants have no incentives—such as lower fees, discounts, or reimbursements—for adopting mobile payments, just more costs. But there is a generalized belief that mobile will "personalize" the retail experience by attracting, identifying, engaging, and rewarding consumers with special offers and loyalty programs. Remember, security has never been the primary motivation for a consumer to adopt a new payment method, but perceived lack of it could prevent the consumer from adopting it in the first place. Recent surveys show that mobile payments might not reach mass adoption until 2020.

Understanding the Operating Systems

The smartphone market is a mixture of Android, iPhone, and Windows devices (which have very low adoption). Apps allow for mobile devices to handle email, web surfing, and calendar management, as well as social media and even video.

Android is the most popular. It offers phone manufacturers and carriers free license to use and modify the core operating system.

Apple's iOS second release opened up the secured environment to apps. When developers use the recommended development tools and languages, this is called "native development." When a developer uses one language in conjunction with tools such as Adobe's PhoneGap, they can build one set of code for many platforms, called "hybrid" solutions. But hybrid struggles to build complex solutions. If you want to build a solution leveraging a new unsupported API, you have to hack a workaround, which raises other issues down the road.

A recent study by Gartner Vice President Joseph Feiman found that "infrastructure and perimeter protection technologies lack insight into application logic and configuration, event and data flow, executed instructions, and data processing." In plain English, they cannot protect against app-level attacks. Feiman says, "Perimeter protection cannot protect as the perimeter dissipates in the mobile, consumer, and Cloud-oriented environment. … There are too many apps, testing skills are scarce, and tools are too complex and inaccurate." The apps should be capable of security self-testing, self-diagnostics, and self-protection, and this is not the case today. This is the real problem.

Protection Beyond EMV

Merchants are supposed to be PCI compliant, based on which of the four levels of size and volume of their transactions. Additionally, processors already have adopted tokenization and end-to-end encryption (E2EE).

Tokenization is a simple concept: Just take the 16-digit card number and replace it with 16 randomly generated letters that can only be used for one transaction. If a fraudster hacks the token, it is useless to them.

E2EE uses algorithms to encrypt the data at the point it enters the system. It is sent as an encrypted message to the processor, which decrypts and authorizes it, and then re-encrypts it and transmits it back to the POS.

When a business cannot authenticate EMV cardholder information in person (a card-not-present transaction), vaulting is an option. Vaulting is a method to establish recurring transactions ("Remember Me") on a merchant's website. The data is stored at the processor, not the merchant.

Risks and Vulnerabilities

One of the big risks with mobile payments is assuming that a secure solution exists when it does not. For example, consumers think that using their "touch ID" (a fingerprint coupled with an alphanumeric password) deters hacks, but there is no central database of fingerprints, other biometrics, or passwords, and anything can be replicated. EMV looks more secure, but initial studies show that consumers often leave their cards in the terminals. The EMV rollout combines chip and signature; there is no PIN number. Of course, the signature is meaningless. Device fingerprinting looks good, but surprisingly large numbers of phones are lost or stolen. IDs without a form factor look appealing, but they do not reach across different banks and merchants. There are vendors that can provide a secure, trusted mobile identity, or a telephone-based, real-time, multifactor, out-of-band authentication.

There are three major vulnerabilities with mobile payments. First is consumer behavior. Consumers lose their phones or leave them where they can be stolen. In addition, consumers often click links in SMS text messages and emails and download third-party apps without any scrutiny.

Second, consumers frequently use third-party apps, which often come from providers who have little or no security practices in place. Unfortunately, some of these apps are created by fraudsters and come preloaded with malware, such as a virus, a Trojan, or rootkits (to enable continued privileged access to a computer).

Third, the unsecured wireless network enables fraudsters to take control of a mobile device and account information.

Preventing Fraud

Fraudsters want data: personal information about cardholders. Ironically, they can buy this type of data on the Internet via a large and sophisticated black market of stolen data, but much of this has already been reported to the card issuers and is useless. Fraudsters want more timely data.

One of the big targets for fraudsters has been PC-based electronic cash registers using integrated POS software. When a merchant is storing a consumer's personal information, there is always a risk of theft.

One recent development, called "secure commerce architecture," enhances security and frees software developers from the PCI process. The introduction of Cloud technologies can ensure seamless and secure payments across multiple channels. There are many vendors in this space, as well as standalone technologies. Very large merchants typically have a security expert on their payroll and employ a variety of vendor solutions, but smaller merchants do not, and are likely more vulnerable.

There are indicia surrounding the transaction that can be used to identify potential hackers—if you have the tools or a vendor-supplied solution. Fraud rates are higher for card-not-present transactions and for transactions from a prepaid phone, so merchants should pay attention to these areas. Try to identify if a mobile device is being used to initiate the transaction, and the type of device. Determine if it is a prepaid device, as this has a higher fraud rate and is the preferred modus operandi for hackers. Determine if the phone number is being forwarded from somewhere else. Any of these things should raise your suspicions regarding a specific transaction, and you would be well served to have a methodology for highlighting suspicious transactions.

Fraudsters will continue to aggressively target mobile transactions with the goal of acquiring personal consumer data that can be used elsewhere. Merchants and ISOs are advised to investigate the vendors in this space that can provide varying levels of protection, and to be vigilant. ***TT***

Brandes Elitch is director of partner acquisitions for CrossCheck Inc.

ADVERTISERS INDEX

Robert K. Rowe

With more than 25 years of experience developing optical products, Robert K. Rowe, PhD, is inventor or co-inventor on more than 60 patents and patents pending for hardware and algorithms related to biometrics and other technology. He is the VP of strategic development, imaging and biometrics, at HID Global and previously co-founded biometrics and smart imaging firm Lumidigm in 2001. Here, he explains how biometrics work.

Which forms of biometric verification work best for payments?

Biometric modalities that are currently used or considered for financial transactions include fingerprint, facial recognition, iris and other eye-related biometrics, voice, and vein biometrics. The best modality for an application varies based on the type of financial transaction—for example retail transactions versus banking—and specific constraints of the deployment. However, any biometric being considered for financial transactions needs to be secure, fast, reliable, and easy to use.

How do they work?

Fingerprint sensors acquire an image of the pattern of the finger pads. Fingerprint images can be collected using different kinds of sensors including ones that measure light, electrical characteristics, or thermal characteristics. In all cases, the fine details of the resulting fingerprint images are analyzed and used for biometric matching.

Facial recognition uses a digital camera of some kind—generally visible or infrared—to acquire an image of a person's face.

Iris sensors acquire an image—generally infrared—of the colored portion of a person's eye, which has fine structure that is unique. The blood vessels and other fine structure in the white regions of the eye may be imaged.

Voice biometrics analyzes the characteristics of a phrase spoken by a person, and vein biometrics uses infrared light to take an image of the shape of the larger blood vessels in fingers or palms.

In all cases, the images or other data are analyzed by computers running sophisticated algorithms. The data from this analysis is matched against similar data that have been collected at an earlier time ["enrollment"]. If the two biometric data sets are sufficiently similar, then authorization for the transaction is granted.

Can't these methods be spoofed?

"Spoofing" is a major concern and area of focus for many biometric professionals. Certain types of biometric sensors, such as multispectral fingerprint sensors, acquire large amounts of information about the material characteristics of anything touching the sensor and can use this information to detect spoofs. Voice recognition systems may use a "challenge-response" method, which requires a person to repeat a random phrase that the biometric system provides, and therefore defeats attempts to use voice recordings of an authorized person.

Some biometric deployments address spoofing concerns by using an additional authentication factor, such as a smartphone or PIN, in conjunction with the biometric. In such cases if there is a concern that both the biometric and the second factor have been copied, then the second factor can be disabled and replaced to restore a certain level of security.

Is the data stored, and what are the ramifications if it is stolen?

Certain types of biometric applications, such as ATM banking, generally store the biometric enrollment data in a secure database and use a tamper-resistant biometric sensor built into the ATM to collect new biometric information each time a person wants to withdraw money or conduct other transactions. Newly collected biometric information is encrypted and securely sent to a back-end computer system to be matched against the information in the enrollment database. If the biometric characteristics match, then another secure message is sent to the ATM to authorize the transaction.

In other types of financial transactions, such as retail purchases, a smartphone may be used to make a transaction after the person authenticates him- or herself to the phone. In the most secure versions of this biometric configuration, a person's biometric information is maintained within a separate tamper-resistant portion of the smartphone and is not transmitted outside of this subsystem. In this way, the opportunities for unauthorized access to biometric data are minimized.

In either configuration, it is imperative that system designers take the proper measures to ensure that biometric information is maintained securely by preventing unauthorized access to the data, encrypting stored data, and following other good security practices.

Note, however, that biometric characteristics are not secrets. For example, our facial characteristics are quite public. Best practices require that solutions are designed to detect the fraudulent use of biometric data. Liveness detection—the determination that the biometric characteristics presented are real and not fake—is one such design feature. ***TT***

—Josephine Rossi

Each Click is a Residual Payment.

Authorize.Net has paid out more residual payments than any other payment gateway. Contact us to learn why.

Call 1.866.437.0491 or visit www.authorize.net

Authorize.Net®
a CyberSource solution

Secure Payments Confidently

With strong encryption and industry proven card authentication inside the reader head, cards and sensitive cardholder data are protected at the very first point of interaction with a MagneSafe™ enabled payment device.

If that's not enough, the data is also dynamically tokenized with every transaction, whether the consumer pays with a secure swipe, a chip, or a mobile phone.

Trust the industry experts to help you fully secure your payment environment.

DynaPro*

- EMV Compliant & Certified
- MagnePrint® Authentication
- P2PE Validated KIF
- NFC-Enabled*

DynaPro Mini**

- Tokenization
- 3DES Encryption
- Bluetooth Mobile**
- Certified to Multiple POS Platforms

FIND OUT MORE 562.546.6467 sales@magtek.com www.magtek.com