Securing Card Payments

Challenges & Opportunities

Julie Hanson
Senior Vice President, Card & Payment Products
ICBA Bancard & TCM Bank, NA

Agenda

Securing Payments

- Landscape
- Chip Technology
- Tokenization
- Authentication: Pin & Beyond

ICBA
Bancard & TCM Bank

Agenda

Securing Payments

- Landscape
- Chip Technology
- Tokenization
- Authentication: Pin & Beyond

JCBA
BANCARD & TCM BANK

Payments Landscape - Payments is the 3rd largest industry

Agriculture
$427b

Utilities
$387b

Payments
$302b

Hotels
$213b

Airlines
$174b

Source: McKinsey & Company, 2014 Payments Map

ICBA
Bancard & TCM Bank

Consumers are changing how they shop…
Connecting through more channels and devices.

New consumer interaction points are growth opportunities…

"Omni-channel"

…but increase the complexity of managing fraud.

IMMEDIACY is VITAL

Food /Beverage

DRIZLY

Tickets

FANDANGO

StubHub!

Transportation

lyft

Music

JCBA
BANCARD & TCM BANK

Digital Wallets & Mobile Payments

	Pay	pay	SAMSUNG pay	Microsoft Wallet
Acceptance	• In app and contactless locations – 2.5M+ acceptance locations in US[1]; Move to browser	• Contactless locations and in-app	• Contactless and 90% of mag stripe locations[9]	• Contactless locations in U.S.
Usage	• Volume estimated to be $10.9 billion in 2015[4] • 12 million users[5]; estimated awareness at 71%[6]	• 5 million users[5]; estimated awareness at 49%[6]	• $500M+ in volume since debut[12] • 5 million users [5]; estimated awareness at 57%[6]	• Beyond HCE – Built for Windows Ecosystem across screens and devices – 300M users across the world, 10s of millions of CoF
Issuer Support	• 1,341 issuers support Apple Pay globally[2]	• 116 issuers support Android Pay globally[7]	• 247 issuers support Samsung Pay globally[10]	• HCE Mobile Wallet Commercial Launch – August 2nd with BAC and U.S. Bank, and possibly PNC and BECU.
Global Expansion	• Canada, China, UK, Singapore, Australia[2] – Additional countries announced: Hong Kong, France, Switzerland[3]	• UK[8] – Additional countries announced: Australia, Singapore	• China, South Korea, Spain, Australia, Singapore[11] – Additional countries announced: Australia, Brazil, Canada, Singapore, UK[12]	

Sources: [1]Apple Q2 Earnings Call, April 2016 (estimated 10M+ contactless locations in countries where Apple Pay launched, representing current opportunity); [2]Apple website, June 2016; [3]PYMNTS, June 2016; [4]Reuters, June 2016; [5]Crone Consulting LLC estimates, as cited by Bloomberg Technology, March 2016; [6]Phoenix Marketing International survey of 3K+ credit card holders, as cited by Digital Transactions, April 2016; [7]Android website, June 2016; [8]Android Official Blog, July 2016; [9]Samsung Pay Master FAQ version 1.41 from Samsung Insights, April 2015; [10]Samsung website, June 2016; [11]Samsung press release *(multiple announcements)*, June 2016; [12]Samsung press release, July 2016

JCBA Bancard & TCM Bank

Digital Wallets – Future Trends

$142B+

in mobile payments in the US by 2019[1]

130%

Growth rate for mobile payments projected in 2016[2]

84%

of consumers most trust their bank for mobile payments[3]

- Adoption of merchant apps, both closed loop (e.g. Starbucks, Walmart Pay) as well as open mobile payment platforms (e.g. Microsoft)
- Recent issuer HCE wallet expansion- anticipate additional issuer apps to enter the market later this year
- Visa recently announced the Visa Digital Commerce App (VDCA), with tokenized contactless payment functionality (PNC for prepaid)
- eCommerce Wallet Tokenization – Visa Checkout is currently enabled for tokenization, however tokenized transactions require merchant and issuer token enablement. In 2017, merchant token enablement will be core to our digital strategy

JCBA Bancard & TCM Bank

Sources: [1]Forrester report, November 2014. [2]eMarketer study, January 2016. Includes point-of-sale transactions made by using a mobile device as a payment method; includes checking in with, scanning, swiping or tapping a mobile device at the point of sale to complete a transaction; excludes purchases of digital goods on mobile devices, purchases made remotely on mobile devices that are delivered later on, and transactions made via tablets. [3]ING International Survey on Mobile Banking, New Technologies and Financial Behaviour, April 2015. Survey population of 14,829 people in 15 countries. All brand names and logos are the property of their respective owners and usage herein July not imply product endorsement or affiliation with Visa.

Security Landscape

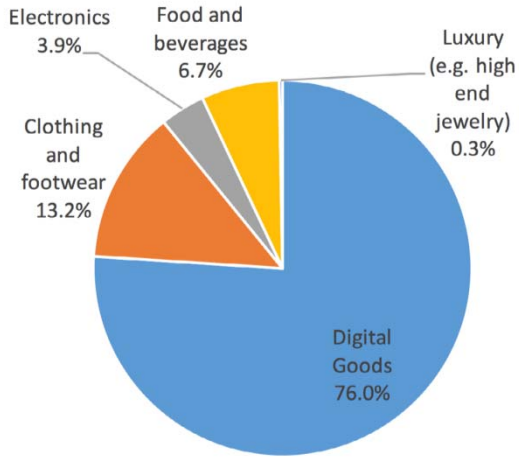
→ Fraud attacks on the US since the October 2015 Liability Shift have increased by 26%

→ Fraud attacks jumped 137% over the last 4 quarters ending March 2016, affecting over $7 out of every $100 made in retail sales

→ Attacks span a wide variety of merchant categories:

- The ***Digital Goods*** industry is the top category targeted by criminals, with ***76%*** of the attacks
- ***Retail*** is second, with ***13.2%***, and
- ***Food*** and beverage is third, with ***6.7%***

WEIGHTED BY NUMBER OF TRANSACTIONS



Source: PYMTS.com 8.30.16-Global Fraud Attack Index Q3 2016

Security Landscape

Payment Card Fraud

→ **Counterfeit fraud** occurs when sensitive account data ***from a magnetic stripe*** card is stolen. This data includes the primary account number (PAN), expiration date and a static card verification code. Because this code is ***static***, as opposed to a dynamic or one-time-use code, it does not offer strong protection against fraud. Once obtained it is used to create a counterfeit payment card.

→ **Card-not-present (CNP) fraud** occurs when the PAN and expiration date ***are stolen or otherwise compromised*** and then used for fraudulent transactions in ***remote-access payment channels***, such as eCommerce, phone/mail orders or recurring payment situations. CNP fraud can result from the harvesting of PAN and expiration date from magnetic stripe **or** chip-read transactions or from remote-payment transactions such as eCommerce.

A Data Breach is an incident in which sensitive, protected or confidential data has been viewed, stolen or used by an individual unauthorized to do so. This data is then used, sold or otherwise shared for purposes of committing payment fraud.

Also known as Botnet fraud (Collections of computers that have been taken over, unbeknownst to the owner, for the purpose of mounting large-scale fraud attacks on retailers) has become the largest method of fraud attacks increasing from 34 to 79 percent globally.

ICBA BANCARD & TCM BANK

Security Landscape

"Employee Assistance"

- 60% of hackers compromise an organization within minutes
- 23% of recipients click on phishing messages
- 11% of recipients click on attachments in phishing messages
- Nearly 50% of recipients open emails and click on phishing links ***within an hour*** of receipt

Training

Institute end-user security awareness

+

Behavior Monitoring

Employ insider behavior monitoring

+

Content Filtering

Stop drive-by downloads

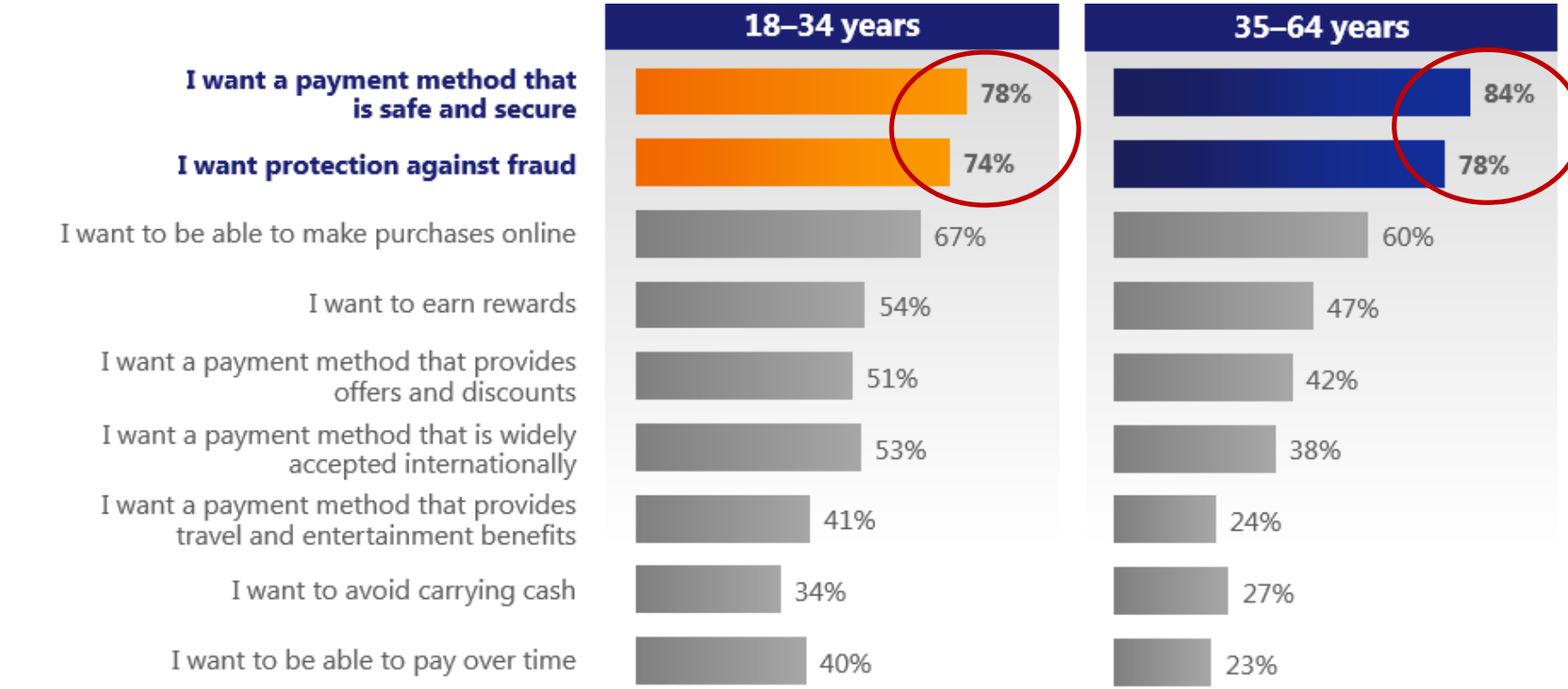
Customer account takeover is a major challenge for financial services and eCommerce organizations. Criminals use credentials stolen from victims via phishing and malware attacks to gain unauthorized access to customers' accounts. Once inside the compromised account, criminals can transfer money, execute fraudulent purchases, or exploit relationships with other customers.

-Ron Andrews, VP and Vertical Leader for Financial Services at Convergys

ICBA Bancard & TCM Bank

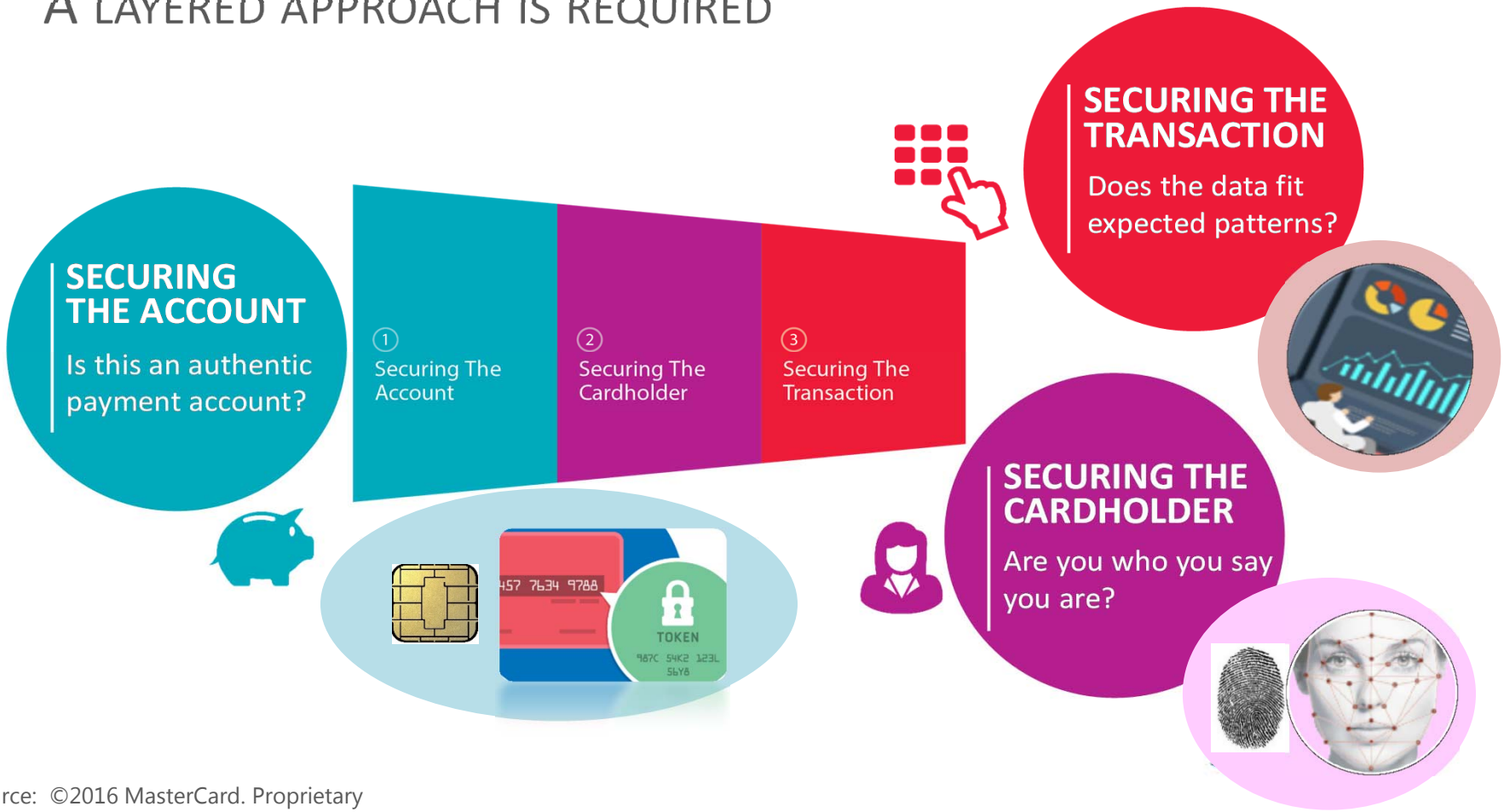
Source: 2016 Q3 PYMNTS Global Fraud Attack Index; Trustwave Global Security Report; Digital Transactions March 2016; ITBusinessEdge

Security Landscape – Payment Security is Important



Note: All responses significantly different between age groups
Source: 2014 Visa Payment Tracker

A LAYERED APPROACH IS REQUIRED



Agenda

Securing Payments

- Landscape
- Chip Technology
- Tokenization
- Authentication: Pin & Beyond

ICBA
Bancard & TCM Bank

Chip Technology

EMV Transaction Flow & Security Measures

1. Card Authentication

Cardholder data resides ***on the chip***, not the mag stripe.

2. Cardholder Verification

Pin vs. Signature: most credit is remaining with signature; online PIN for debit. Offline verification can be done via information stored on the chip.

3. Transaction Authorization

Online authorization includes a transaction-specific, one-time code called a ***cryptogram*** which is virtually impossible to replicate

ICBA Bancard & TCM Bank

EMV – Where are we now?*

Chip Cards Issued:

Visa (7/30/16): **171.4M** credit cards
174.5M debit cards

MasterCard (5/30/16): **78%** of US-issued MC consumer credit cards
26% of US-issued MC consumer debit cards

Usage:

Visa: **26.1%** of US credit and **10.5%** of US debit card chip-on-chip transactions
MasterCard: **15%** of monthly POS transactions and **21%** of Payment Volume

Fallback Rate: Visa: **2.9%** for US EMV credit card and **5.1%** US EMV debit card
MasterCard: **2.0%** of POS transactions were processed as fallback

Merchant locations:

Total: **1.38M** Visa and **1.6M** MC Chip-active merchant locations

Counterfeit Fraud Decrease: Visa: **38%** in April compared with April 2015; MC: **33%** Jan '15- 'Jan 16

* Visa Stats as of June 30, 2016 & MC Stats as of May 30, 2016 – unless otherwise noted

Sources: Visa, MasterCard and Digital Transactions

ICBA Bancard & TCM Bank

EMV – Where are we now?

ICBA
Bancard & TCM Bank

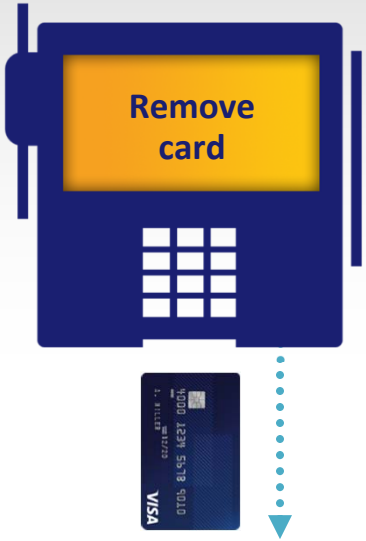
Quick Chip - How is works at the POS

Insert the card face up, chip end first

1

Remove card when prompted. Processing should take 2 seconds or less

2



Follow prompts on screen to finalize transaction

3

JCBA
Bancard & TCM Bank®

POS = Point-of-Sale

Visa Quick Chip; MasterCard M/Chip Fast

Agenda

Securing Payments

- Landscape
- Chip Technology
- Tokenization
- Authentication: Pin & Beyond

ICBA
Bancard & TCM Bank

Tokenization

Tokenization is the practice of replacing sensitive data such as an account number with a unique, digital identifier called a **token**. If this substitute value or "token" is stolen, the criminal's ability to use it for fraudulent transactions is removed.

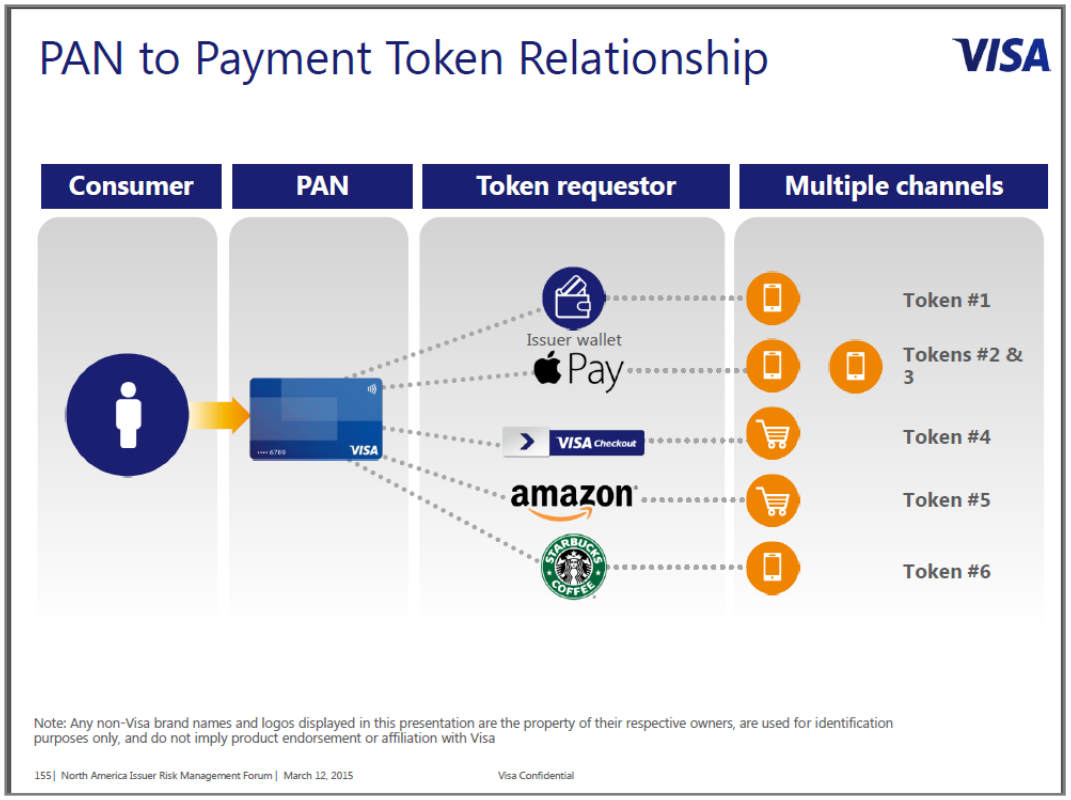
Benefits:

- The tokenization process happens in the background in a way that is invisible to the consumer.
- Reduces fraud in **e-commerce and m-commerce transactions** by removing sensitive card account information (account number) from the payment process. If obtained, the data is useless to fraudsters.
- Tokens ensure that the sensitive data is not transmitted or stored by a merchant in an unsecure format. Therefore, they can be retained by online merchants or on mobile devices to facilitate ecommerce and mobile payments.

Definition Source: Payments Security Taskforce

ICBA
Bancard & TCM Bank

Tokenization

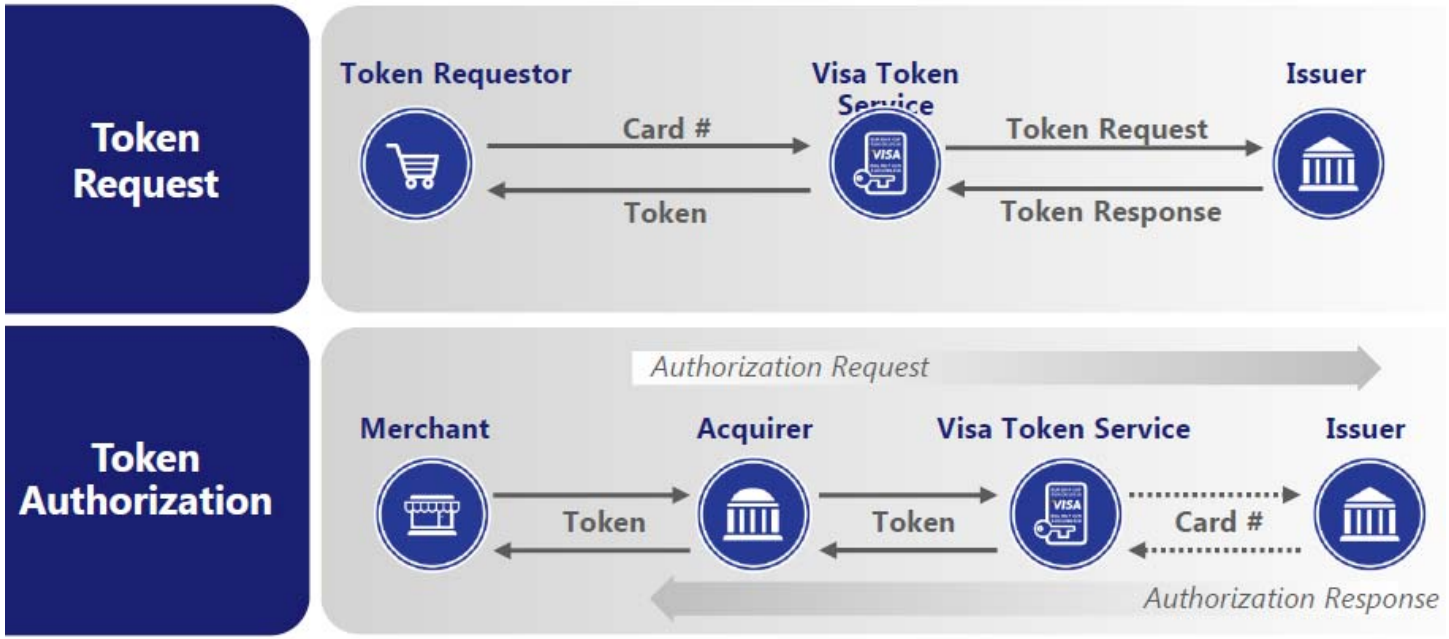


The **P**rimary **A**ccount **N**umber is changed into a token and tokens vary by merchant.

ICBA Bancard & TCM Bank

Tokenization

Token Request *(provisioning)* and Authorization Processes



Source: Visa North American Issuer Risk Management Forum, March 12, 2015 *Confidential*

Agenda

Securing Payments

- Landscape
- Chip Technology
- Tokenization
- Authentication: Pin & Beyond

ICBA
Bancard & TCM Bank

Authentication

There are three primary ways in which a customer can authenticate his or her identity:

1. Ownership factor – Something a person has, like a credit card or other physical token.
2. Knowledge factor – Something the person knows, like a PIN or password.
3. Inherence Factor – Something the person is or does, like a fingerprint or unique facial features.

Biometrics (inherence) factors such as fingerprints and retinal scans have their pros and cons:

- Pro: can ensure and protect the cardholders' identity
- Pro: cannot easily be counterfeited as they are unique to the customer and are easily accessible
- Pro: authentication information is not retained by the merchant
- Con: is costly to implement
- Con: is less convenient for consumers and usually requires a longer time commitment for the checkout process as the merchant is requiring an additional factor of authentication.

ICBA
Bancard & TCM Bank

To PIN or not to PIN

To assure a smooth transition to EMV cards, major card brands are not mandating the use of PINs.

Why not?

- None of the major recent data breaches at U.S. retailers—such as Home Depot and Target—were caused by customers using payment cards without PINs, and none of these breaches would have been prevented by customers using cards with PINs.
- A PIN, like a signature, is a form of authenticating a user, but it is also static data element, which can make it vulnerable to theft.
- The merchant community is requesting PIN usage not simply for security but for a lower cost routing option. In fact the OCC noted that "although PINs may reduce fraud in certain circumstances, they do not eliminate it. Further, chip-and-PIN may not be adequate for card-not-present transactions, such as those occurring online or via telephone."

ICBA
Bancard & TCM Bank

VISA ALERTS – Engaging the customer

Effective October 14, 2016, Visa will require all U.S. issuers to provide credit, debit, and reloadable prepaid cardholders an option to enroll in transaction alerts (Non-reloadable prepaid and commercial card excluded). Issuers may provide their own alerts service or offer one from a third party, such as their processor, a mobile application developer, or Visa.

How it works:
To receive Visa alerts, cardholders must first sign up for the service through their participating issuer. Once enrolled, cardholders can set up specific alert triggers that meet their individual account information needs. Anytime a transaction takes place that meets the cardholder's defined parameters, he or she receives an alert in "near" real time.

Triggers can include: • Transaction thresholds for spending amount • International transactions • Card-absent transactions, such as telephone or Internet orders • Declined transactions • ATM cash withdrawals • Gasoline charges

Benefits: • Strengthen customer relationships • Enhance your competitive position • Reduce fraud exposure and associated losses • Expand new customer relationships • Increase brand and value awareness • provides consumer peace of mine

Consumers who receive transaction alerts experience 40% less fraud than account holders who do not.

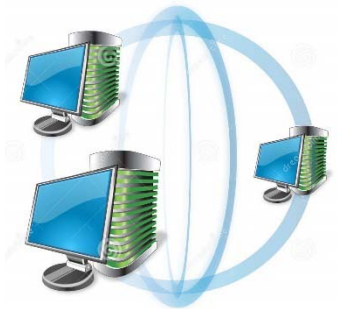
JCBA
Bancard & TCM Bank

Network-Based Monitoring

Network-based monitoring systems use data analytics, neural networks, transaction risk scoring, anomaly detection and custom rule-based decsioning to identify and prevent fraud.

Benefits:

- Can process events, develop strategies to detect fraud and create cases, and execute associated decisioning across card transactions or across payment channels
- Adds an additional layer for fraud detection and prevention



With MasterCard's ***"SafetyNet"*** and Visa's ***"Predictive Fraud Analytics***", each uses advanced fraud monitoring and detection systems to prevent fraud.

In less time than it takes for the receipt to print out, Visa analyzes and risk scores every transaction it processes – *more than 61 billion annually* – and provides intelligence to help merchants and financial institutions identify fraud and stop it in its tracks.

ICBA
Bancard & TCM Bank

Point-to-Point Encryption

Point-to-Point Encryption (P2PE) is a payment security solution that protects payment data as it travels through payment systems (terminal/merchant ➡ network/processor).

At card swipe it converts confidential credit card data and information into ***indecipherable code*** to thwart hacking and mitigate fraud. It encrypts payment data in a secure terminal and transmits it through an internal or external network where it is decrypted in a secure environment.

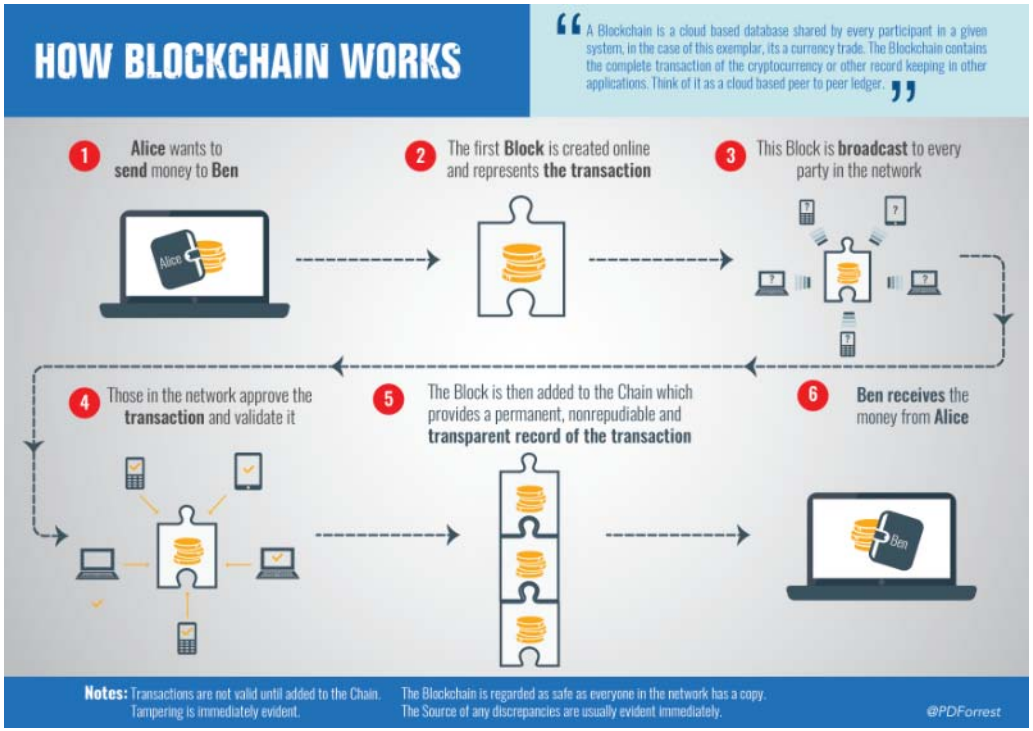
Benefits:

- P2PE significantly reduces the risk of credit card fraud by ***instantaneously*** encrypting confidential cardholder data at the moment a credit card is swiped.
- The data can't be read and reused if it is stolen or compromised.
- The payment process with P2PE is faster than other transaction processes creating simpler and faster customer-merchant transactions.

ICBA
BANCARD & TCM BANK®

Blockchain

Blockchain is a series of blocks that hold timestamped batches of valid transactions. Each block includes the hash of the prior block in the Blockchain which creates the link. The linked blocks then form a chain with only one block allowed to link to another.



JCBA
Bancard & TCM Bank

Summary

- The way in which consumers transact is multi-faceted and ever growing "Omni-channel"
- The need for *multiple*, secure technologies to reduce the ever-resent secur threats is necessary
- One form of technology alone isn't going to mitigate the risk or actual fraud
- Help your customers and merchants understand that we need their help in embracing new forms of transacting and processing in order to deliver safe solutions
- Don't get too comfortable….technology will continue to evolve ☺

ICBA
Bancard & TCM Bank

Thank you!

Julie Hanson
Senior Vice President, Card & Payment Products
ICBA Bancard & TCM Bank, NA