

ILLINOIS COMMUNITY COLLEGES

CFO CONFERENCE SPRING 2015

April 9, 2015

PAYMENT INDUSTRY TRENDS AND UPDATES

This presentation was prepared exclusively for the benefit and internal use of the J.P. Morgan client or potential client to whom it is directly delivered and/or addressed (including subsidiaries and affiliates, the "Company") in order to assist the Company in evaluating, on a preliminary basis, the feasibility of a possible transaction or transactions or other business relationship and does not carry any right of publication or disclosure, in whole or in part, to any other party. This presentation is for discussion purposes only and is incomplete without reference to, and should be viewed solely in conjunction with, the oral briefing provided by J.P. Morgan. Neither this presentation nor any of its contents may be disclosed or used for any other purpose without the prior written consent of J.P. Morgan.

To the extent that the information in this presentation is based upon any management forecasts or other information supplied to us by or on behalf of the Company, it reflects such information as well as prevailing conditions and our views as of this date, all of which are accordingly subject to change. J.P. Morgan's opinions and estimates constitute J.P. Morgan's judgment and should be regarded as indicative, preliminary and for illustrative purposes only. In preparing this presentation, we have relied upon and assumed, without independent verification, the accuracy and completeness of all information available from public sources or which was provided to us by or on behalf of the Company or which was otherwise reviewed by us. J.P. Morgan makes no representations as to the actual value which may be received in connection with a transaction nor the legal, tax or accounting effects of consummating a transaction. Unless expressly contemplated hereby, the information in this presentation does not take into account the effects of a possible transaction or transactions involving an actual or potential change of control, which may have significant valuation and other effects.

Notwithstanding anything herein to the contrary, the Company and each of its employees, representatives or other agents may disclose to any and all persons, without limitation of any kind, the U.S. federal and state income tax treatment and the U.S. federal and state income tax structure (if applicable) of the transactions contemplated hereby and all materials of any kind (including opinions or other tax analyses) that are provided to the Company insofar as such treatment and/or structure relates to a U.S. federal or state income tax strategy provided to the Company by J.P. Morgan. J.P. Morgan's policies on data privacy can be found at <http://www.jpmorgan.com/pages/privacy>.

IRS Circular 230 Disclosure: JPMorgan Chase & Co. and its affiliates do not provide tax advice. Accordingly, any discussion of U.S. tax matters included herein (including any attachments) is not intended or written to be used, and cannot be used, in connection with the promotion, marketing or recommendation by anyone not affiliated with JPMorgan Chase & Co. of any of the matters addressed herein or for the purpose of avoiding U.S. tax-related penalties.

Chase, JPMorgan and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, "JPMC") and if and as used herein may include as applicable employees or officers of any or all of such entities irrespective of the marketing name used. Products and services may be provided by commercial bank affiliates, securities affiliates or other JPMC affiliates or entities. In particular, securities brokerage services other than those which can be provided by commercial bank affiliates under applicable law will be provided by registered broker/dealer affiliates such as J.P. Morgan Securities LLC or J.P. Morgan Institutional Investments Inc. or by such other affiliates as may be appropriate to provide such services under applicable law. Such securities are not deposits or other obligations of any such commercial bank, are not guaranteed by any such commercial bank and are not insured by the Federal Deposit Insurance Corporation. Not all products and services are available in all geographic areas. Eligibility for particular products and services is subject to final determination by JPMC and or its affiliates/subsidiaries.

This presentation does not constitute a commitment by any JPMC entity to extend or arrange credit or to provide any other services.

After today's session you'll better understand ...

- The current payment/commerce climate
 - Complexity of payments
 - Security, Fraud and Compliance differences
- Payment technology and methods of payment
 - ApplePay and Mobile Wallets
 - Mobile
 - Alternative Payments (PayPal and ECP)
- Security Fraud Tools and Solutions
 - Encryption Services (card present and not-present environments)
 - Tokenization (P2P and E2E)

Payment Climate today

Businesses are challenged like never before

Payments are becoming
Complex

- More complicated rules, regulations and rate tables
- Security concerns requiring new tools
- Global card acceptance, evolving regulations and conventions
- Mobile retailing growth (70%) surpassing retail (4.2%) in 2013

Cost
is rising for payment acceptance

- Cost of payment acceptance continues to grow
- New payment types represent new fees
- Infrastructure enhancement costs required to meet data security
- Potential losses – The total cost of payment card fraud was nearly 14 billion in 2013¹

Elusive
Growth

- Growth challenges
- Shifting cardholder preferences
- Technology creating challenges

Businesses are losing
Control

- EMV Chip and PIN introduced by October 2015
- New PCI 3.0 mandates underway
- Windows XP is end-of-life
- Tablets and smartphones dominate Internet connections

¹The Nilson Report, BI Intelligence 2014
Note: Nilson Report ranking largest merchant acquirers for 2013

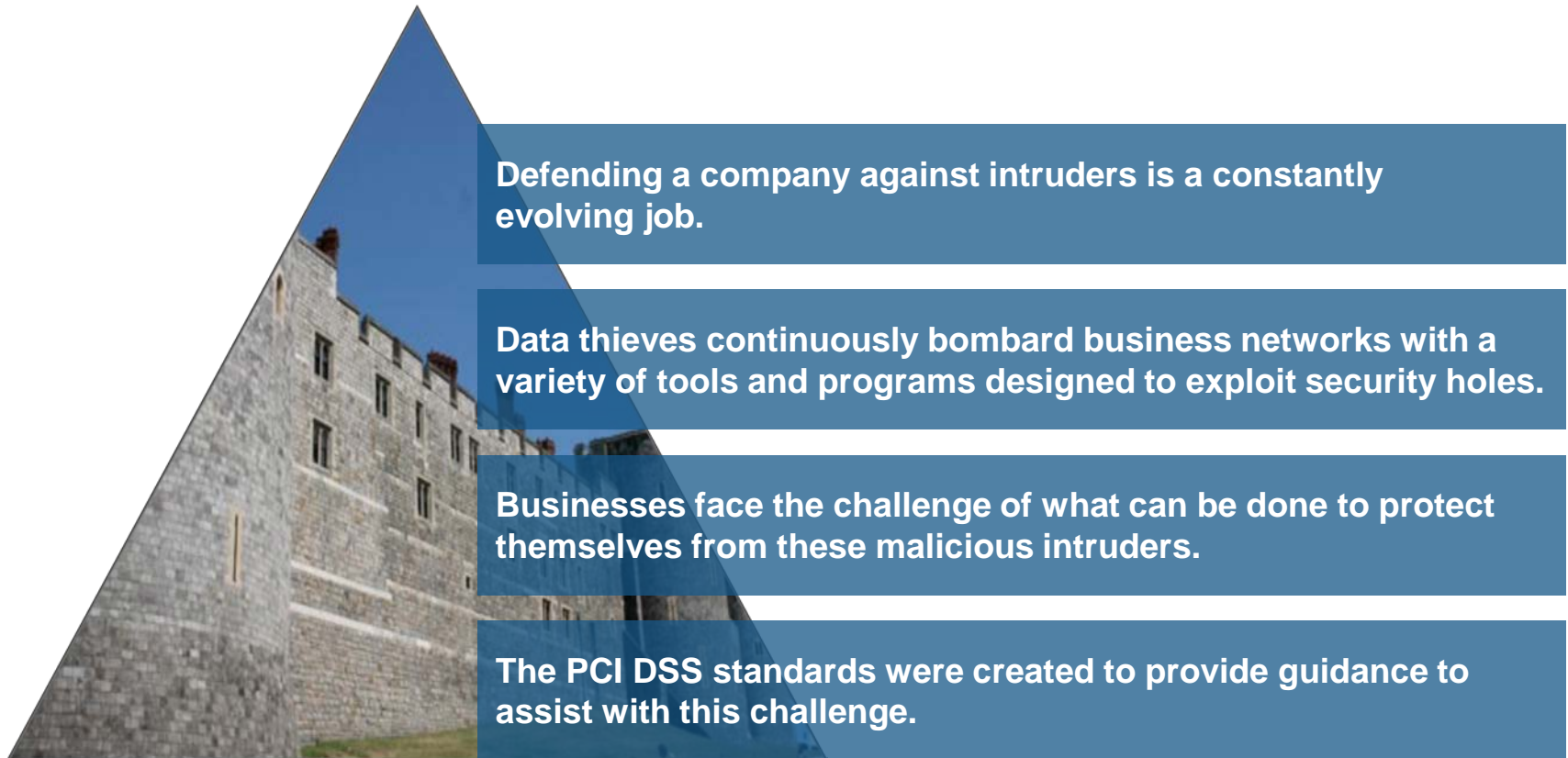
Costs of a breach

Category	Description	Company A: Low-profile breach in a non-regulated industry (\$)	Company B: Low-profile breach in a regulated industry (\$)	Company C: High-profile breach in a highly regulated industry (\$)
Discovery, notification and response	<ul style="list-style-type: none"> Outside legal counsel, mail notification, calls, call center and discounted product offers 	50	50	50
Lost employee productivity	<ul style="list-style-type: none"> Employees diverted from other tasks 	20	25	30
Opportunity cost	<ul style="list-style-type: none"> Customer churn and difficulty in getting new customers 	20	50	100
Regulatory fines	<ul style="list-style-type: none"> FTC, PCI, SOX 	0	25	60
Restitution	<ul style="list-style-type: none"> Civil courts may ask to put this money aside in case breaches are discovered 	0	0	30
Additional security and audit requirements	<ul style="list-style-type: none"> The security and audit requirements levied as a result of a breach 	0	5	10
Other liabilities	<ul style="list-style-type: none"> Credit card replacement costs Civil penalties if specific fraud can be traced to the breach 	0	0	25
Total cost per record (millions)		90	155	305

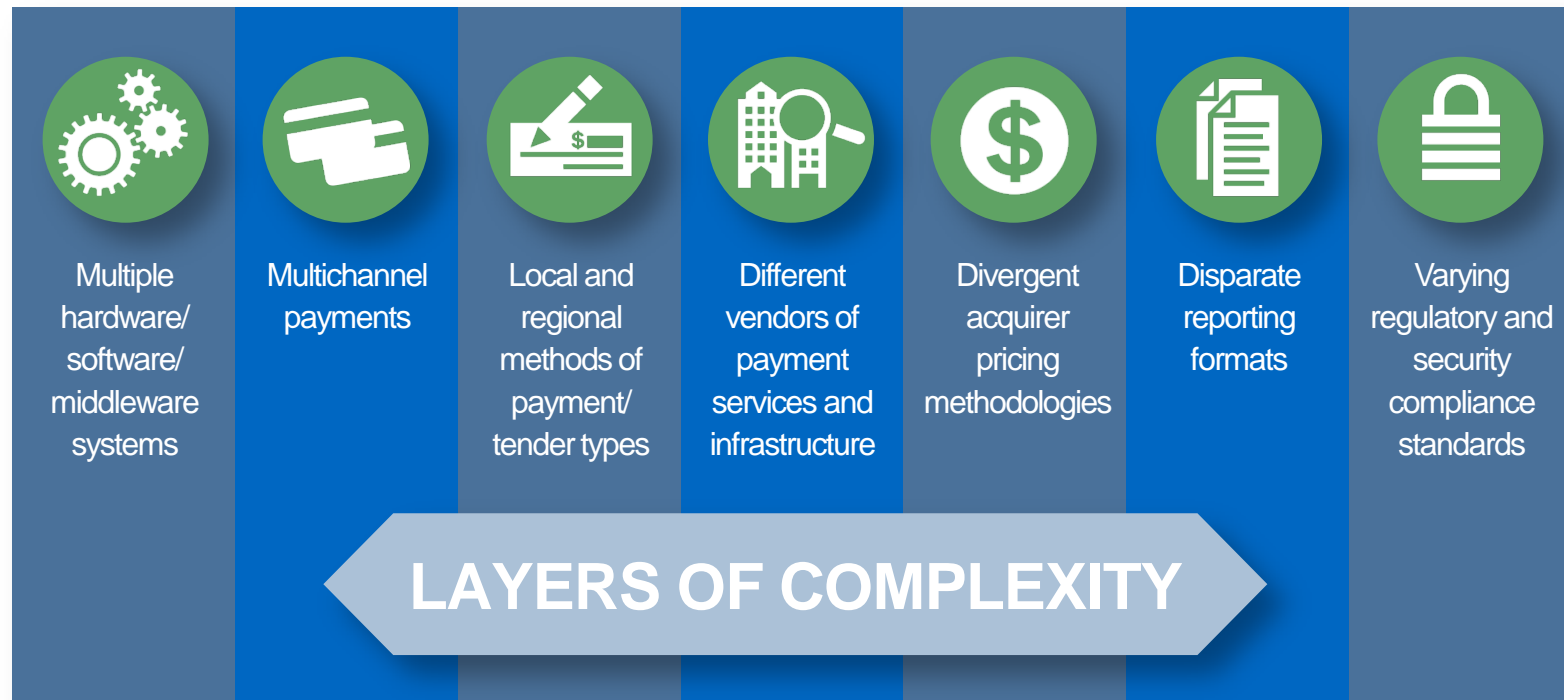
- Example: Initial costs for the TJX breach were \$240 million, with an additional \$36 million in each subsequent year since the breach

Source: Forrester Research

The challenge ... *defend the castle!*



Potential hidden risks in the payment value chain



“It is tough to maintain command and control over your business if you contract outsiders who contract more outsiders who contract additional outsiders.”

– AML expert **Kevin Sullivan**, former investigator with the New York State Police assigned to the NY High Intensity Financial Crimes Area (HIFCA) Task Force

PCI in summary

- A collective term used to refer to the Payment Card Industry Security Standards Council (PCI SSC)
 - Various data security standards developed and maintained by this entity and payment brands with which businesses must comply
- Applies to any system that stores, processes or transmits cardholder data as part of authorization or settlement of a branded credit or debit transaction
- 12 requirements covering operational and technical components
- Specific guidelines available for implementing mitigating technologies such as encryption and tokenization

Applicability

- PCI DSS applies to any system or environment that accesses, stores, processes or transmits cardholder data.
- The PCI DSS defines a series of controls and requirements that are designed to protect cardholder data.

Payment Card Industry Data Security Standard (PCI DSS) Compliance

Guidance, expertise and a wide range of solutions for clients that help with compliance and mitigate operation and financial risk by ensuring that PCI requirements are met.

How your payment partner should help

- Ongoing education and resources
- Various solutions that help manage cost and complexity of compliance
- Preferential pricing with a QSR to help access and validate PCI compliance
- Dedicated resources focused on PCI



PCI DSS requirements

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords and security parameters
- Protect stored data and regularly update anti-virus software
- Encrypt transmission of cardholder data and sensitive information across public networks
- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and implement processes and a policy that addresses information security

Industry standards for fraud prevention

With support of multiple payment brand-approved fraud standards, you can minimize the risks and costs associated with fraud.

Common industry standards we support

- **American Express CID** – Card Identification Number (CID) Fraud Reduction Program reduces card fraud by requiring the sales representative to key the CID number at the point of sale or requires the cardholder to key in the CID number for Internet transactions.
- **Visa CVV2** – Card Verification Value 2 (CVV2) is a three-digit code on the back of a Visa card that follows the card number. This three-digit value provides a cryptographic check of the information embossed on the card or stored within the magnetic strip.
- **Discover CID** – Discover has developed the Cardmember Identifier (CID) Fraud Reduction Program, which reduces card fraud by requiring the sales representative to key the CID number at the point of sale or requires the cardholder to key in the CID number for Internet transactions.
- **MasterCard CVC2** – Card Validation Code 2 (CVC2) is a three-digit code on the back of a MasterCard card that follows the card number. This value provides a cryptographic check of the information embossed on the card or stored within the magnetic strip.
- **Address Verification** – Address Verification Service is provided by the major card networks to combat fraud on card-not-present transactions. The credit card billing address is requested with and verified before authorization is given for the transaction.
- **Verified by Visa and MasterCard SecureCode** – Verified by Visa and MasterCard SecureCode are designed to increase cardholder and client confidence in online purchases and reduce disputes and fraudulent activity related to the use of Visa/MasterCard payment cards.



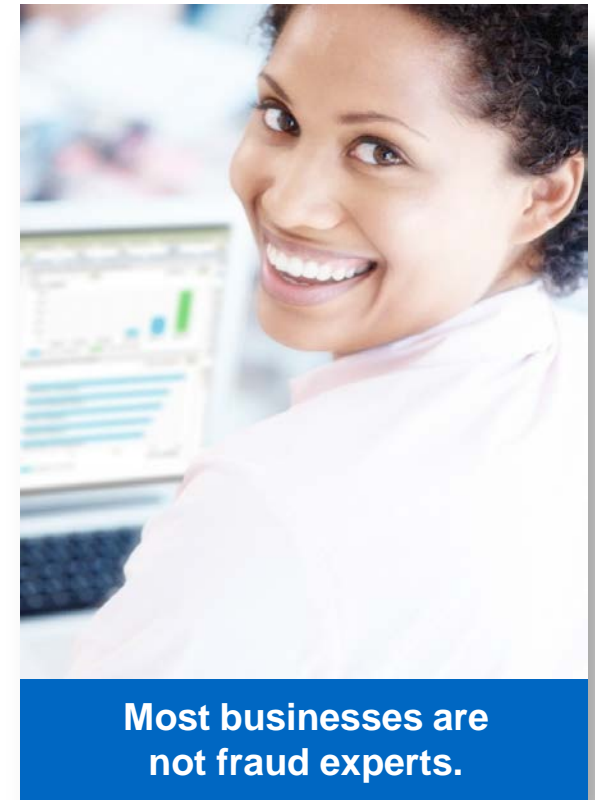
When including lost business and customers, negative branding, etc., every dollar lost to cybercriminals through fraud in reality cost merchants \$2.79, up 10 cents from 2012.¹

¹Source: 5th Annual LexisNexis® True Cost of FraudSM Study, 2013

The reality of fighting fraud

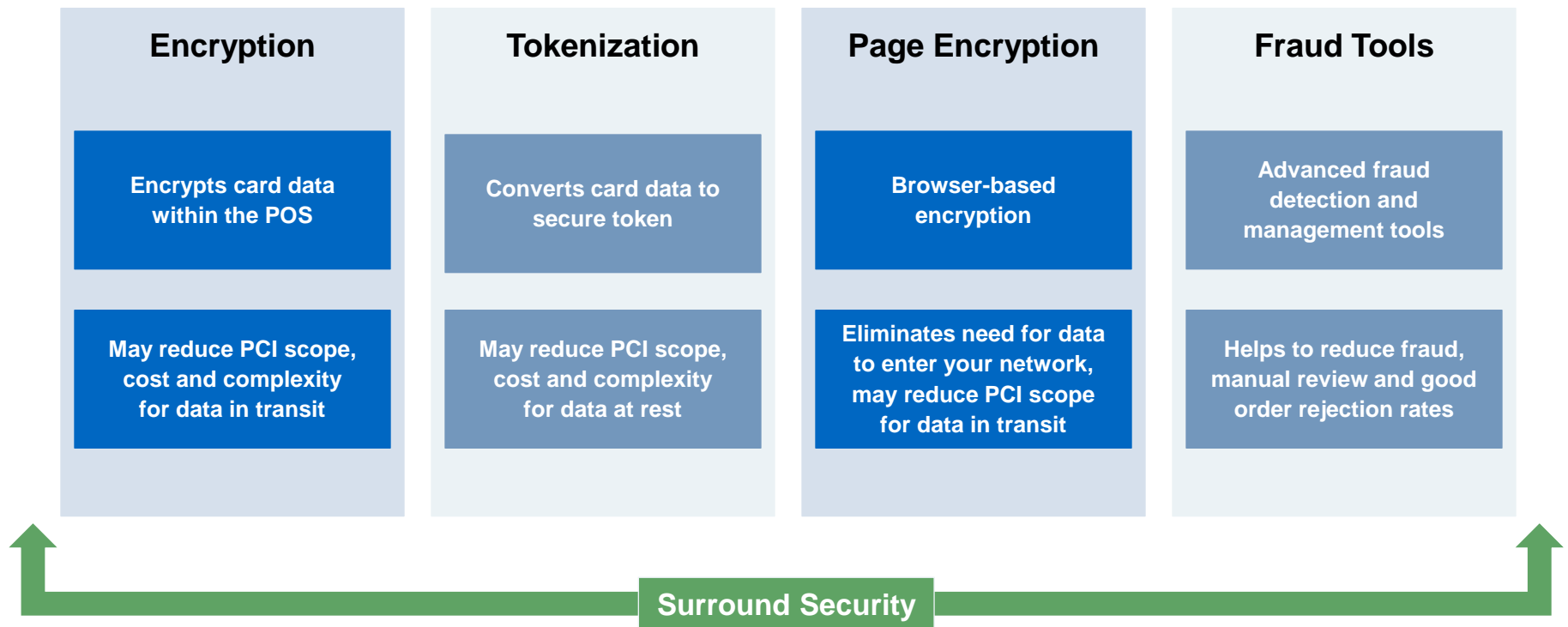
What businesses face

- Businesses are trying to simultaneously protect their bottom line as well as their customers from fraud
- A business might use as many as **eight** tools that are not necessarily interconnected
- Manually reviewing suspect transactions is costly and time consuming when not managed correctly
- A business may not realize they are victims until they get their chargeback reports – *30-90 days after the transaction*
- Fraudsters are nimble and quick, constantly identifying ways to exploit a business' weakness



Security and Fraud Solutions

A comprehensive suite of data protection and fraud prevention tools that streamlines your payments management to help meet your processing, fraud prevention and data security requirements



Note: Integration decisions may impact availability of some of these solutions

Payment brands lay groundwork with EMV

Incent dual interface

- **10/12** Visa will offer PCI validation relief through their Visa TIP program for merchants who process at least 75% of their Visa transactions through a contact/contactless EMV device
- **10/12** MasterCard will offer merchant exemption from annual PCI DSS compliance validation for merchants who process at least 75% of their MasterCard/Maestro transactions through a contact/contactless EMV device
- **10/13** Discover will grant annual PCI audit waivers to merchants who process at least 75% of their contact/contactless Discover Network transactions through a contact/contactless EMV device
- **10/13** AMEX will offer a similar PCI DSS annual validation program

Mandate chip processing

- **04/13** Visa/Interlink, MasterCard/Maestro, AMEX and Discover will all require acquirers to support acceptance of EMV contact/contactless chip transactions through their host platforms in the U.S. region
- **10/13** PULSE will require U.S. acquirers to support EMV data
- **04/14** SHAZAM will require U.S. acquirers to support EMV data
- **10/14** SHAZAM will require U.S. issuers to support EMV

Invoke liability shift

- **10/15** (2017 for AFD) Visa, MasterCard, Discover and AMEX have announced upcoming liability shifts. Any merchants OR issuers who do not support chip technology may be liable for the cost of counterfeit fraud
 - MasterCard will also enforce a liability shift for lost/stolen/never received fraud

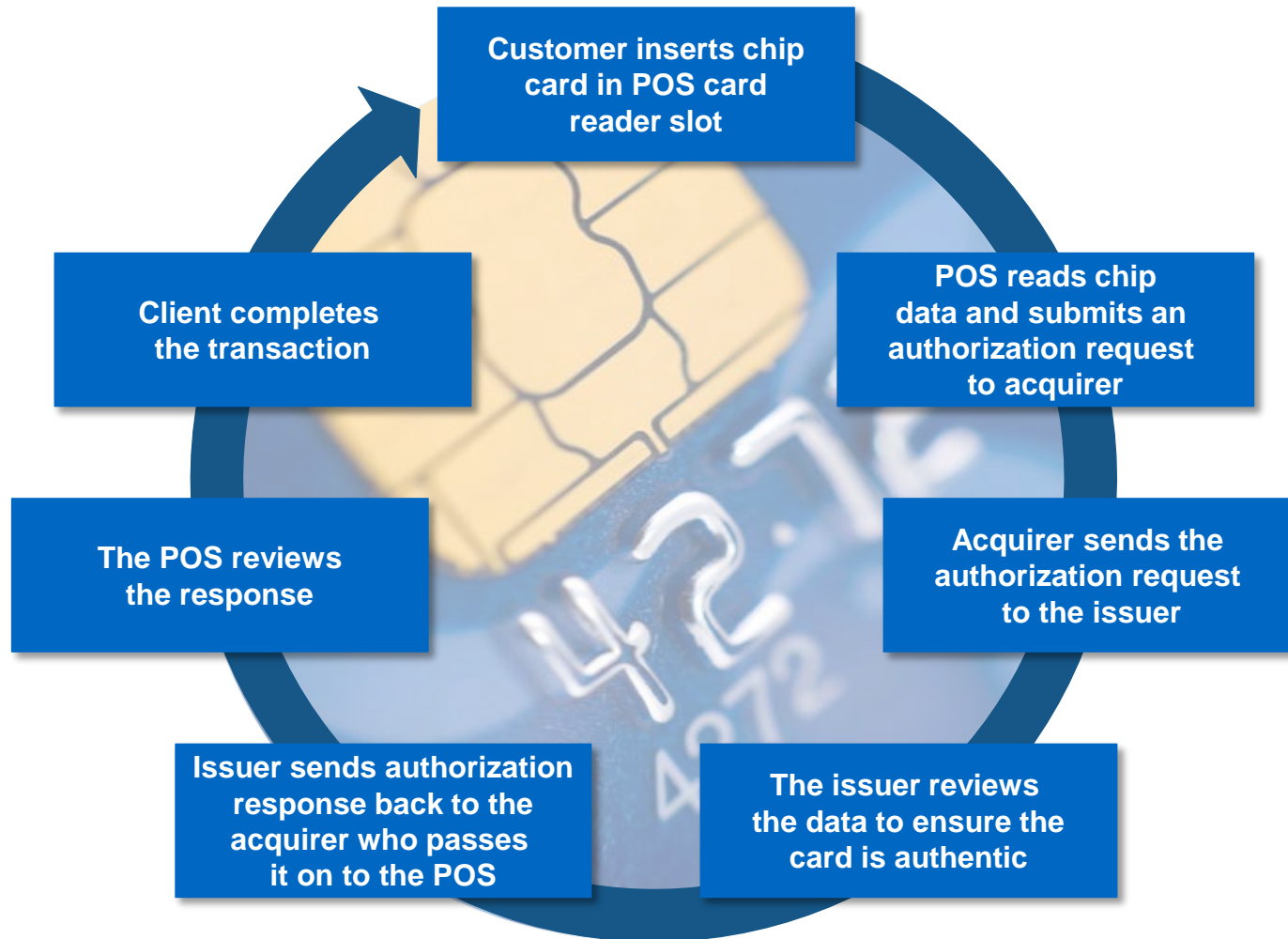
EMV card processing

EMV benefits

- Prevents counterfeit fraud
- Prevents skimming
- Chip instead of magnetic stripe
- NOTE: not a security solution; does not encrypt data



Chip card transaction flow



There are approximately 2.37 billion EMV payment cards in circulation and 36.9 million EMV terminals active worldwide.

Page Encryption and Tokenization

Page Encryption and Tokenization protects cardholder data at the point-of-sale and reduces compliance and security concerns by encrypting it throughout the lifecycle of the transaction – and keeping out of your system.

Page Encryption

- Page Encryption is a scalable data protection solution that enables ecommerce clients to protect primary account numbers (PAN) and sensitive authentication data. The data is captured and secured in the customer's Web browser before it ever reaches your system.

Tokenization

- Tokenization is a service that replaces customer payment data with an alpha-numeric character string that cannot be converted back to card or account information within your network, protecting that data from security threats.

Benefits

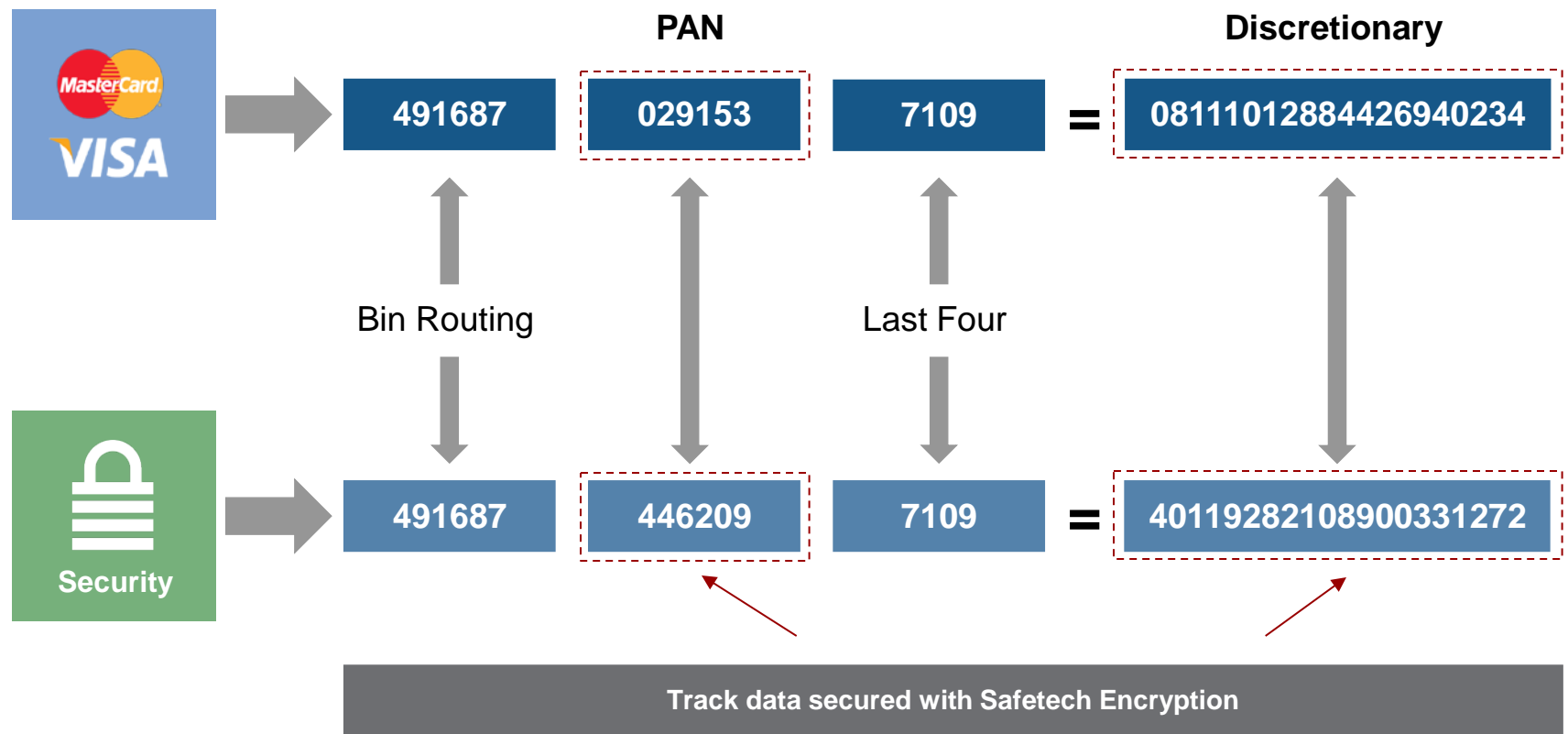
- Secure customer payment data throughout the payment cycle
- Potentially reduce the cost, complexity and scope of PCI compliance
- Minimize impacts to IT resources
- Maintain complete control of your website branding and transaction data throughout the payment cycle, enabling you to perform analytics, testing and updates as needed
- Reduce the need to store cardholder data

How it works

- Page Encryption uses JavaScript to encrypt the PAN and data entered on the pay page within the customer's browser
- Data is sent to your service provider/acquirer, through the client network
- Your service provider/acquirer decrypts the PAN and card security code and seeks authorization
- Your service provider/acquirer sends the authorization response and token to the client

Encryption - How it works

Track data is encrypted at the point of sale (contactless, swiped and manually entered). An algorithm reformats the data so the POS system processes it in the same manner as previously unencrypted data. This reformatted PAN data passes the MOD 10 check



Tokenization highlights

Tokenization

- A service that replaces customer payment data with a benign value that cannot be converted back to card or account information within a client's network, protecting that data from security threats



- Multiple encryption and tokenization options:
 - Format-Preserving Encryption (FPE)
 - Embedded Format-Preserving Encryption (eFPE)
 - Format-Preserving tokenization
 - Numeric formats
 - Obvious token formats (forced alpha character)
- Tokenization available without page encryption
- Reporting displays token value, not clear card number
- Transaction history supports token search:
 - Supports historical reference to all incidences of card use
- Tokenization may sometimes be available for retail processing integration

Combining technology = more protection

Page Encryption

- Secure data capture
- Data is not stored

Tokenization

- Data capture in the clear
- Secure data storage

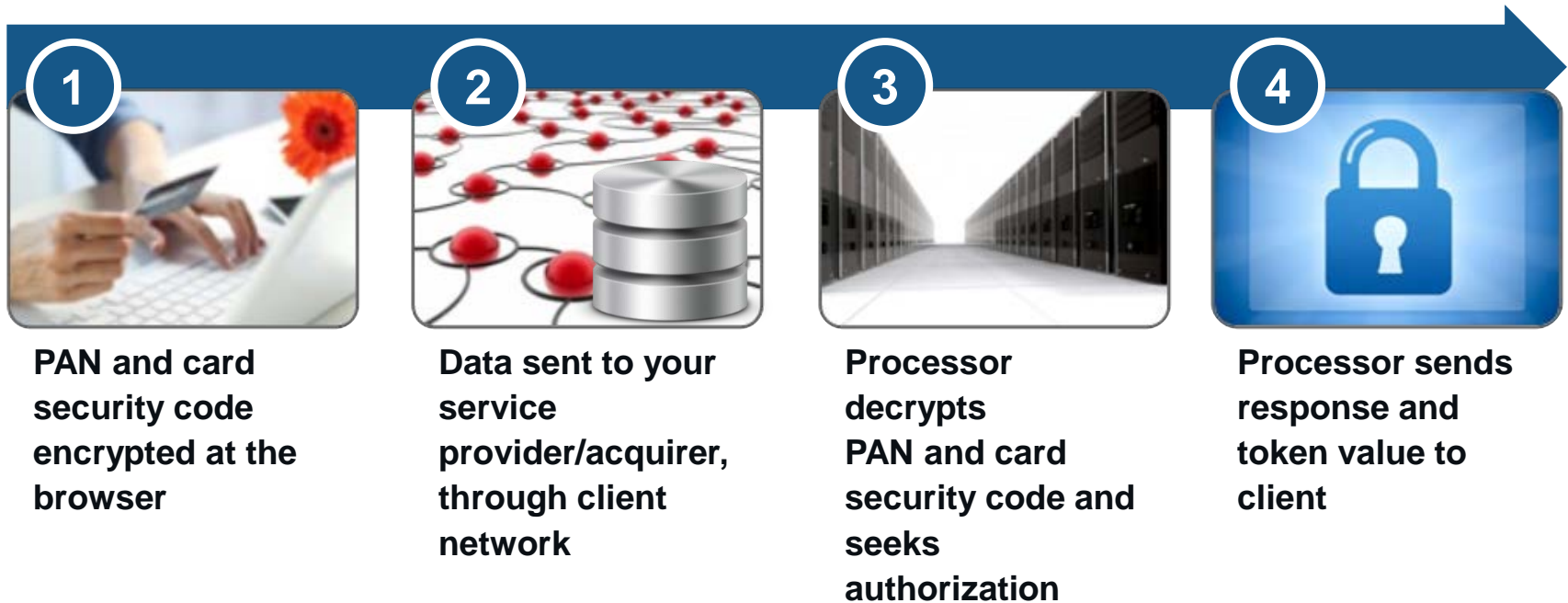
Secure data capture and storage

A combined solution provides greater benefit

Removing exposure of card data may reduce the risks typically associated with a compromise

Reducing risk has the benefit of reducing PCI scope

... with simple results



- Client system is not exposed to payment card data in the clear
- No ability to decrypt at the client location

Alternative payments

Alternative methods of payment are fully integrated with credit and debit card payment processing, funding and reporting. These methods help grow sales by increasing payment choices available to customers.

PayPal



- PayPal enables any individual or business with an email address to send and receive payments online securely, easily and quickly.
- Through some service providers clients receive full support of PayPal Express Checkout. This allows consumers to expedite the checkout process because PayPal provides the consumer's shipping information so the consumer does not need to fill it in at the client's checkout page.

PayPal Credit, formerly known as Bill Me Later



- PayPal Credit, a PayPal company, is a simple, secure, convenient payment option that card-not-present clients can offer to their consumers.
- PayPal Credit allows clients to offer to their customers a better buying experience while enjoying increased sales, a higher average order value and repeat usage, while lowering transaction costs.
- PayPal Credit, a PayPal Company, partners to provide this service to clients in the direct response and ecommerce markets.

Mobile Devices



- Ability to securely accept payments on the go with a secure card reader and device with Wi-Fi or cellular service

NOTE: ALWAYS protect customer data with point-to-point encryption and the proper security measures

What is PayPal Credit?

- PayPal Credit (formerly Bill Me Later) is a leading alternative electronic payment option among top retailers online, with more than 30 of the Top 100 Internet Retailer ecommerce companies offering the service:
 - Credit granted or denied at the point of sale
 - An alternative to credit cards
 - Available promotional pricing
 - No consumer application or set credit limit
 - Ideal for catalog, mail order, telephone order and Internet use

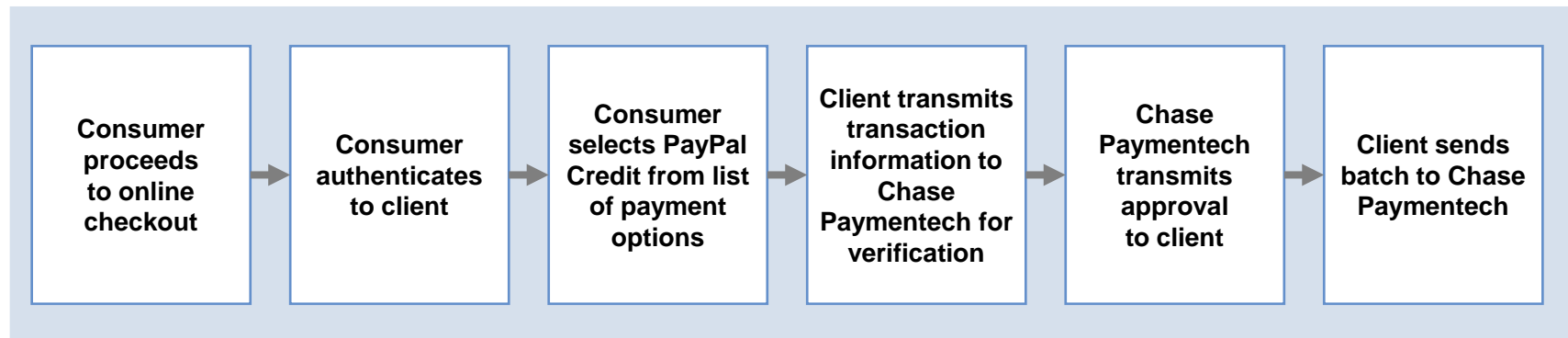


As a credit account, PayPal Credit can provide your customers the flexibility to purchase without using a credit card.

Requesting a PayPal Credit account is quick, easy and secure. Customers simply select PayPal Credit at checkout to complete the request.

How PayPal Credit (formerly Bill Me Later) works

- Clients present PayPal Credit as a method of payment, either online or over the phone
- Each transaction request is reviewed and approved based on PayPal Credit risk criteria, which includes proprietary credit scoring, fraud detection tools and credit reporting services
- Previous PayPal Credit shoppers are authenticated
- Decisions are rendered online in three to five seconds




Apple Pay

Apple Pay is an innovative mobile wallet that delivers high security, easy acceptance and enhanced customer experience at the point of sale and in the mobile app.

Client benefits	Apple Pay features	<p><i>“JPMorgan Chase has been pleased to collaborate on Apple Pay to create a better, faster and safer payments system, which puts the customer first, creating an exceptional customer experience for consumers and merchants. Everyone wins.”</i></p> <p><i>– Jamie Dimon, Chairman and CEO, JPMorgan Chase & Co.</i></p>
<ul style="list-style-type: none"> ■ Increased payment security ■ Simplified, fast checkout ■ Enhanced customer experience ■ Potentially reduced PCI compliance 	<ul style="list-style-type: none"> ■ Designed for in-person retail and in-app transactions ■ Uses advanced tokenization, encryption and biometric security techniques to protect data ■ Apple Pay supports credit and debit cards from the three major payment networks (American Express, MasterCard and Visa) issued by the most popular banks including Chase and representing 83 percent of credit card purchase volume in the U.S.¹ 	


How it works

Retail



- User waves iPhone near an NFC-enabled terminal and places a finger on Touch ID to make the payment.
- Client accepts Apple Pay on a qualifying NFC-enabled terminal using their existing acquirer.
- Tokenized payment is processed as an EMV contactless transaction. No additional coding or integration is required.

In-App



- Client integrates Apple Pay into its mobile app with the easy-to-use Chase SDK or their own programming. Features Apple Pay logo as a payment option at checkout.
- Customer chooses Apple Pay for payment in the app and places a finger on Touch ID to complete the transaction.

¹Apple press release, September 9, 2014

The experts like Apple Pay



“... With the recent news of the credit card breaches from Target and Home Depot, iPhone users could see Apple Pay as a safer payment alternative. And if you don’t offer Apple Pay, you could be losing out on these customers’ payments.”

– Stuart Parkerson, Sept. 16, 2014



“Why Apple Pay could be the mobile-payment system you’ll actually use.”

– Rich Mogull, Sept. 12, 2014



“Analysts: Apple Pay will help spur wider usage of mobile payments”

“... Apple will prove effective at marketing mobile payments to consumers, not as a technology but as something that will make paying for goods and services with your phone fast, easy and even fun...”

– Phil Goldstein, quoting Ovum analyst Eden Zoller, Sept. 10, 2014

Questions



Jeanie Griffin, Director - Business Development
Chase Paymentech
Office: 630.554.2984
Jeanie.Griffin@chasepaymentech.com