WISCONSIN GOVERNMENT FINANCE OFFICERS ASSOCIATION

PROCUREMENT CARDS & FRAUD

Sheniece Syas / Brian McGoldrick
JPMorgan Chase
Commercial Card Fraud Prevention

September 24, 2015 | OCONOMOWOC, WI

CHASE

J.P.Morgan

Fraud Overview

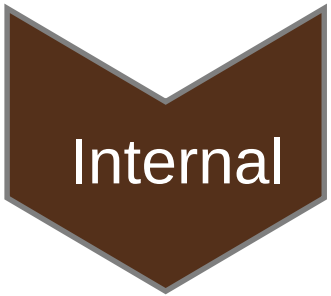
Sheniece Syas

Fraud Overview Session Content

- What is Fraud
- Methods of Stealing Card Information
- Current Industry Trends
- Fraud Department Structure
- Client Best Practices

What is Fraud

- Also known as third party fraud
- Transaction(s) not authorized
- Fraud made with a lost, stolen or counterfeit card or stolen account information



- Also known as employee misuse
- Transaction(s) made with a company administered credit card for personal gain by an employee or contractor of the company
- Spend or activity is outside the parameters of the company policy

Methods of Obtaining Fraud Information

Breach

- Data Compromise at the Merchant or a Merchant Processor

Compromise

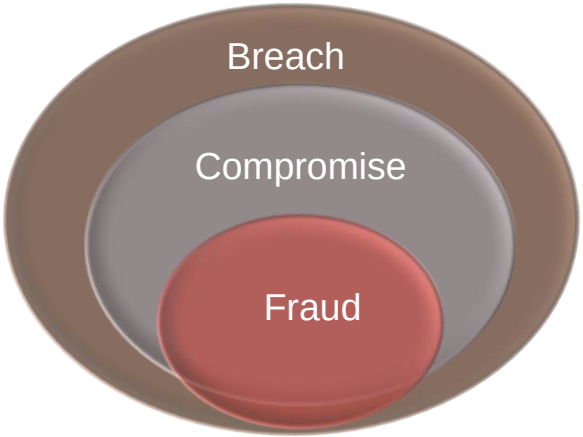
- Account data is in the possession of people with malicious intent

Fraud

- Confirmed non-authorized use of an account

Magnetic Stripe Data

- Card Number
- Name
- Expiration Date
- PIN Verification Data: defines and decrypts PIN
- Card Verification Value – CVV: unique identifier to specific card



CHASE

J.P.Morgan

Types of Breaches

1. **Processor Weakness**
   - Merchant networks are accessed using: malicious software
2. **Skimming**
   - Device placed on merchant terminal (card reader) that captures magnetic stripe data
3. **Credit Master**
   - Perpetrators use automated and/or manual methods to figure out an algorithm that allows them to generate and test valid account numbers and expiration dates
4. **Phishing**
   - Perpetrators gain access to critical systems by tricking the merchant or cardholder into providing confidential security credentials
5. **Theft at a Merchant**
   - Stolen computer equipment i.e. laptop, thumb drive, etc.

CHASE

J.P.Morgan

Fraud Types

- **Lost or Stolen** – Recoverability varies depending on circumstances
- **Card Not Present** – Mail Order Telephone Order (MOTO) / Internet - Recoverability of loss is very good
- **Counterfeit / Card present** – Recovery through chargeback process less likely
- **Non-receipt of card** – not as common due to activation requirements on cards
- **Account takeover** – True name fraud

Current Industry Trends

- **Gift Cards** – Counterfeit card used to purchase gift cards from a retail merchant
- **Bad Merchants** – Create fake businesses with “low risk” merchants to create quick transactions
- **Day to Day Living Expenses** – Not as easily detected in the tools
- **Gas Pumps** – fraud increases when price of gas increases
- **Counterfeit Fraud** – One of the fastest growing forms of fraud
- **Credit Master Schemes** – Process to find valid account number and expiration dates
- **Test Merchants** – Method in which fraudsters test the status of the card prior to sale or use

Fraud Department Structure

- Analyze fraud trends
- Adjust fraud tools and strategies
- Review false positive fraud ratios
- Participate in industry fraud meetings
- Analyze & ID potential points of compromise

- Analyze accounts in fraud queues 24/7
- Contact cardholders to validate transactional activity
- Process replacement cards
- Report potential Misuse Opportunities

- Consult clients on best program controls to mitigate fraud risk
- Assist clients in disaster situations
- Work with law enforcement
- Monitor & manage industry compromise activity

- Open fraud cases
- Send Affidavit/ Confirmation Email
- Request & initiate chargeback recovery
- Refer suspicious activity for potential SAR filing

CHASE

J.P.Morgan

Best Practices in Fraud Prevention

Card Control Utilization

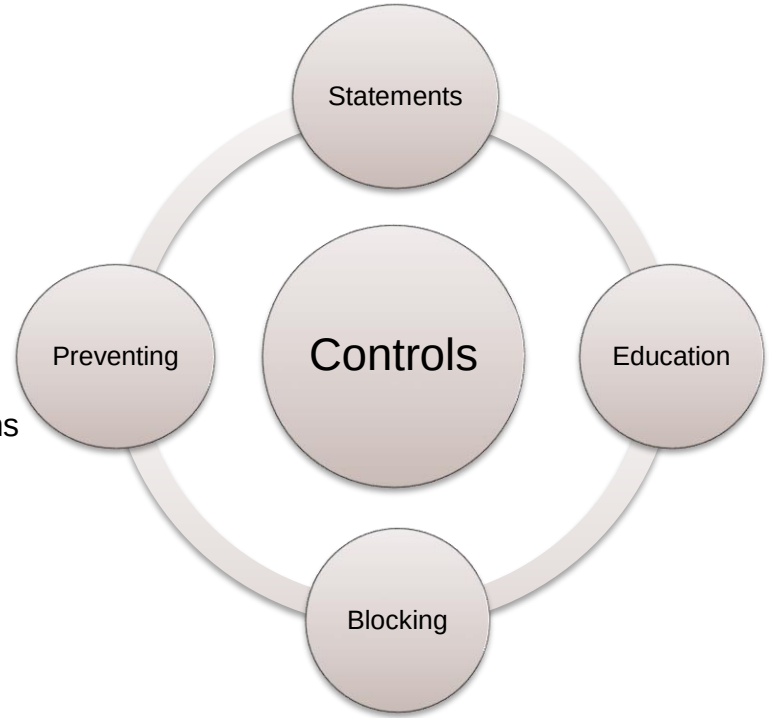
- Implement velocity limits on MCCs & Completely close MCCs not needed
- Review and set credit limits based on usage
- Limit cash access & Review International usage

Educate your cardholders to:

- Review their transactions and statements
- Immediately report lost or stolen cards or fraud transactions

Use account blocking for temporary leaves or infrequent travelers

- Notification of Voluntary/Involuntary terminations



CHASE

High Risk Merchant Category Codes

- Fraud trends are always changing, but the list below provides a current snapshot of consistently targeted Merchant Category Codes
  - 5310 Discount Stores
  - 5411 Grocery Stores and Supermarkets
  - 5200 Home Supply Warehouse
  - 5941 Sporting Goods
  - 5311 Department Stores
  - 5541 Service Station
  - 5542 Automated Gas Pump
  - 5912 Drug Store and Pharmacy (Gift Cards)
  - 5732 Electronic
  - 5944 Jewelry Watch and Clocks
  - 5945 Hobby Toy and Game Store
  - 5948 Luggage and Leather Goods
  - 5722 Household Appliances
  - 5300 Wholesale Clubs
  - 5734 Computer Software
  - 4812 Telecommunication Equipment Including Telephone Sales
  - 6051 Non-Financial Institutions —Foreign Currency, Money Orders, and Travelers Cheques

CHASE

J.P.Morgan

Chip Card

Brian McGoldrick

Chip Card Basics

Chip Reader

Chip-embedded

Chip terminal

Chip & PIN

Chip Card

Smart Card

Chip-enabled

Chip technology

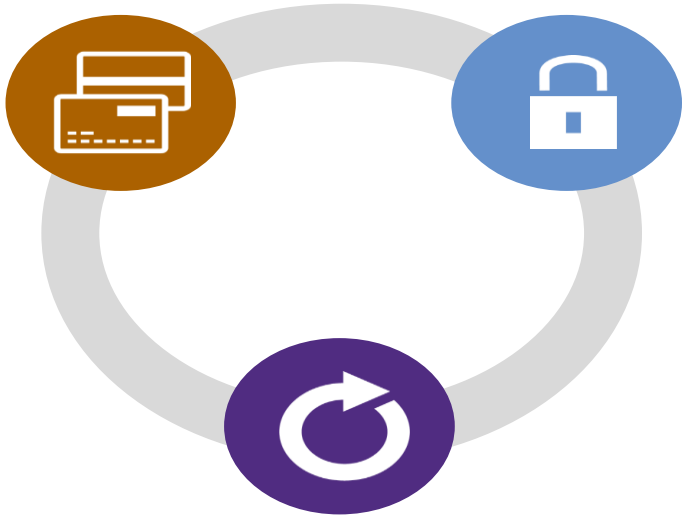
Chip & Signature

EMV

Evolving Payment Landscape

Credit Card Fraud

- Card skimming
- Counterfeiting



Account Information Security

- Protecting personal information

Acceptance Issues

- New technology adoption

The evolving landscape has driven the need for enhanced payment technologies, such as chip

CHASE

J.P.Morgan

Chip Card (EMV) Decrease In Fraud

Country/Area	Year EMV First Implemented	Fraud Decrease
Australia	2008	▪ 38% decline in counterfeit fraud from 2008 to 2010*
Canada	2008	▪ 54% decline in counterfeit and lost or stolen fraud from 2008 to 2013*
France	1986	▪ 50% decline in fraud in domestic, face-to-face transactions from 2004 to 2009*
United Kingdom	2004	▪ 55% decline in counterfeit fraud and 33% decline in lost or stolen card fraud from 2005 to 2013*

CHASE

* [5] "EMV Lessons Learned and the US Outlook," Aite Group, June 2014. (Via the Australian Payments Clearing Association).
[6] Ibid.(Via Canadian Bankers Association)
[7] "Chip and PIN, Successes and Failures in Reducing Fraud
[8] "EMV Lessons Learned and the US Outlook." (Via Financial Fraud Action UK).

J.P.Morgan

Trends towards Chip Technology

- Card payment standards are evolving
- Today, there are over 2 billion active chip payment cards with access to over 35 million chip-enabled payment terminals
- Chip Card payment terminals are standard in Canada, Mexico, and most countries in South America, Europe and Asia
- The U.S. is one of the few countries that have not yet fully transitioned, but Chip Cards are expected to become the standard as merchants invest in the technology
- Networks are also promoting an industry shift to chip technology, specifically the October 2015 liability shift

Source: EVMco, A Guide to EMV Chip Technology, V 2.0 November 2014

CHASE

J.P.Morgan

Chip Card Basics

Chip Cards contain an embedded microchip which has the capacity to store information securely

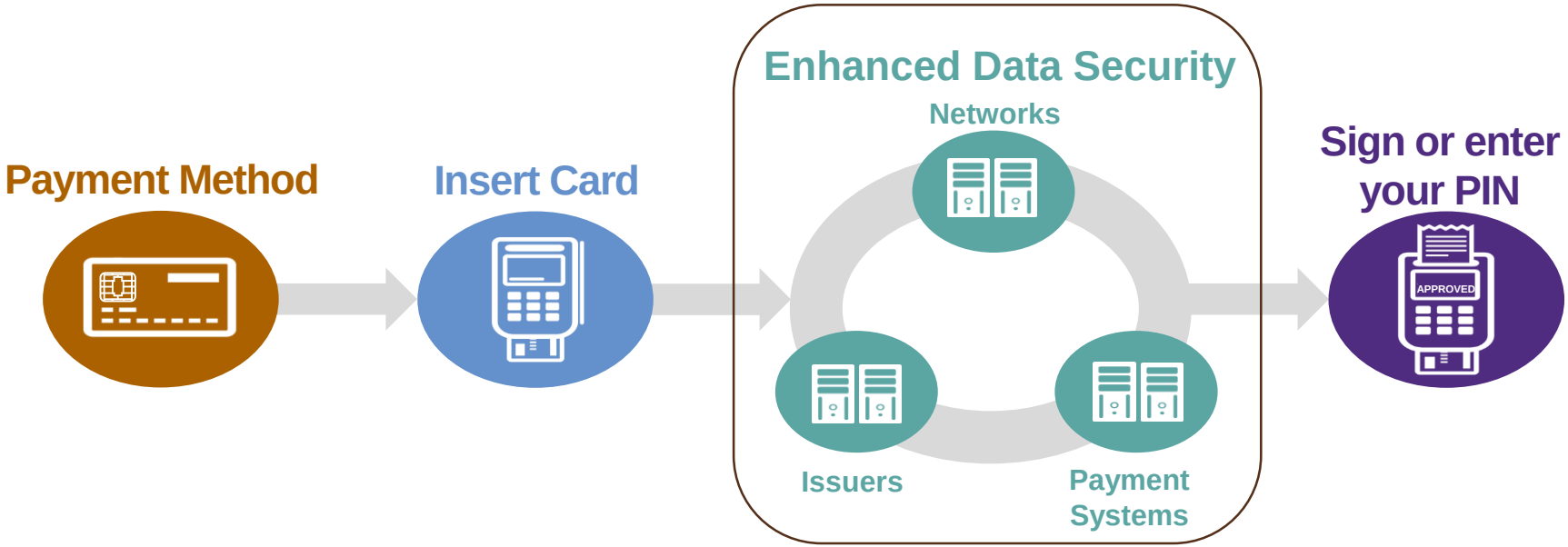
- Improves security for payments at chip terminals*
- Features to help reduce counterfeit fraud*
- Promotes broader acceptance and flexibility*
- Cardholders who travel internationally are able to use Chip Cards at more locations*

**Source: EVMco, A Guide to EMV Chip Technology, V 2.0 November 2014*

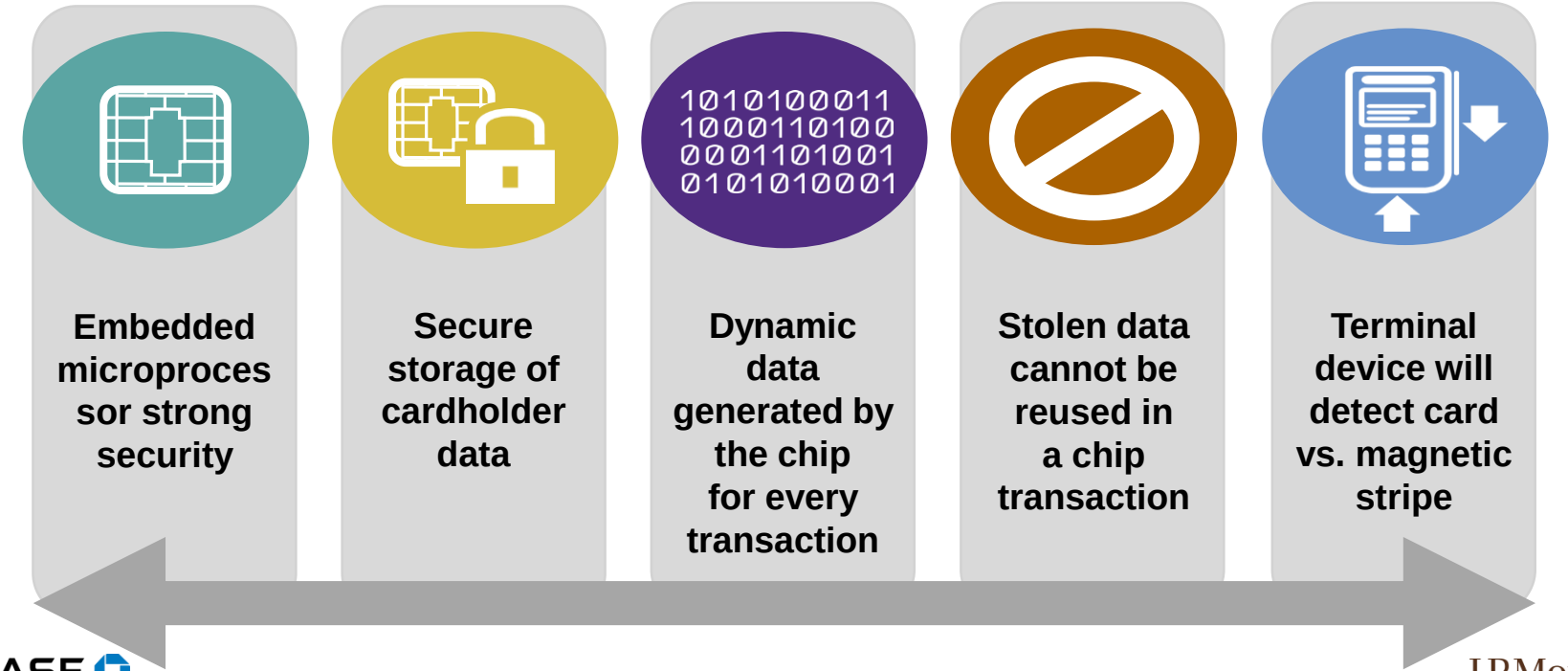
CHASE

J.P.Morgan

How Chip Cards Work



How Chip Technology protects against in-person counterfeit card fraud



CHASE

J.P.Morgan

Chip Card Liability Shift Targeted for October 2015 in the U.S.

What is happening as a result of the Chip Card Liability Shift?

- Transactions where counterfeit card fraud occurs because of the transaction, the party who was least able to support/accept/process the transaction in a chip-compliant manner will be liable for fraud losses

What are the impacts?

- Adoption of chip technology in the U.S. is accelerated by payment networks due to liability shift rule changes

Who is impacted?

- Card issuers and merchants

Who is not impacted?

- Cardholders
- Card not present transactions

CHASE

J.P.Morgan

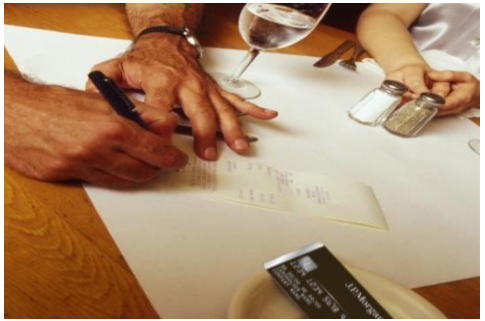
Our Chip Cards

Our Chip Card is built to promote broad acceptance*, leveraging both signature and PIN authorization methods

Three methods:

1. **Swipe With Signature**

2. **Chip With Signature**



3. **Chip With PIN**

Additionally, phone and Internet transactions will work the same way they do today

**Source: EVMco, A Guide to EMV Chip Technology, V 2.0 November 2014*

CHASE

J.P.Morgan

Using a Chip Reader

Insert your card with the chip facing up. Keep in mind that not all chip readers look the same.

Keep it in the card reader, and follow the prompts on the screen to complete your purchase.

If a signature is required, just sign, and always remember to take your card when you're done.

You will continue to sign for most purchases at U.S. and international chip readers. You may only be prompted to enter your PIN for purchases at self-service locations, i.e. train ticketing kiosks, fuel pumps, etc. If you have an issue making a purchase with your PIN, please try your PIN multiple times or find an attendant to help you complete the purchase.

Source: EVMco, A Guide to EMV Chip Technology, V 2.0 November 2014; EMVCo.com, smartcardalliance.org and emv-connection.com

CHASE

J.P.Morgan

Fraud EMV Preparation

What Changes October 1st – Liability Shift

- **In-Store counterfeit fraud liability will shift to the party (either the issuer or merchant) that has not adopted chip technology.**
  - *Note - Fuel Pumps & ATM transactions are unchanged until 10/17*
- As issuers / merchants adopt chip technology counterfeit fraud will decrease and card not present fraud will increase
- Current trend is higher counterfeit fraud % due to compromise activity and increased fraud attacks prior to full chip rollout

Issuer Has	Merchant Has	Fraud Liability
Chip Card	**Non Chip Terminal**	**Merchant**
Chip Card	Chip Terminal	Issuer
Non Chip Card	**Chip Terminal**	**Issuer**
Non Chip Card	Non Chip Terminal	Issuer

Training

- Prevention & Recovery training completed including association training

Strategy

- Analysis performed to include new POS entry modes

Technology

- Verified by Visa tool and Falcon Fraud Predictor implemented

Readiness

- Scorecards developed to monitor chip / non-chip & fallback to magstripe fraud

CHASE

J.P.Morgan

Thank You