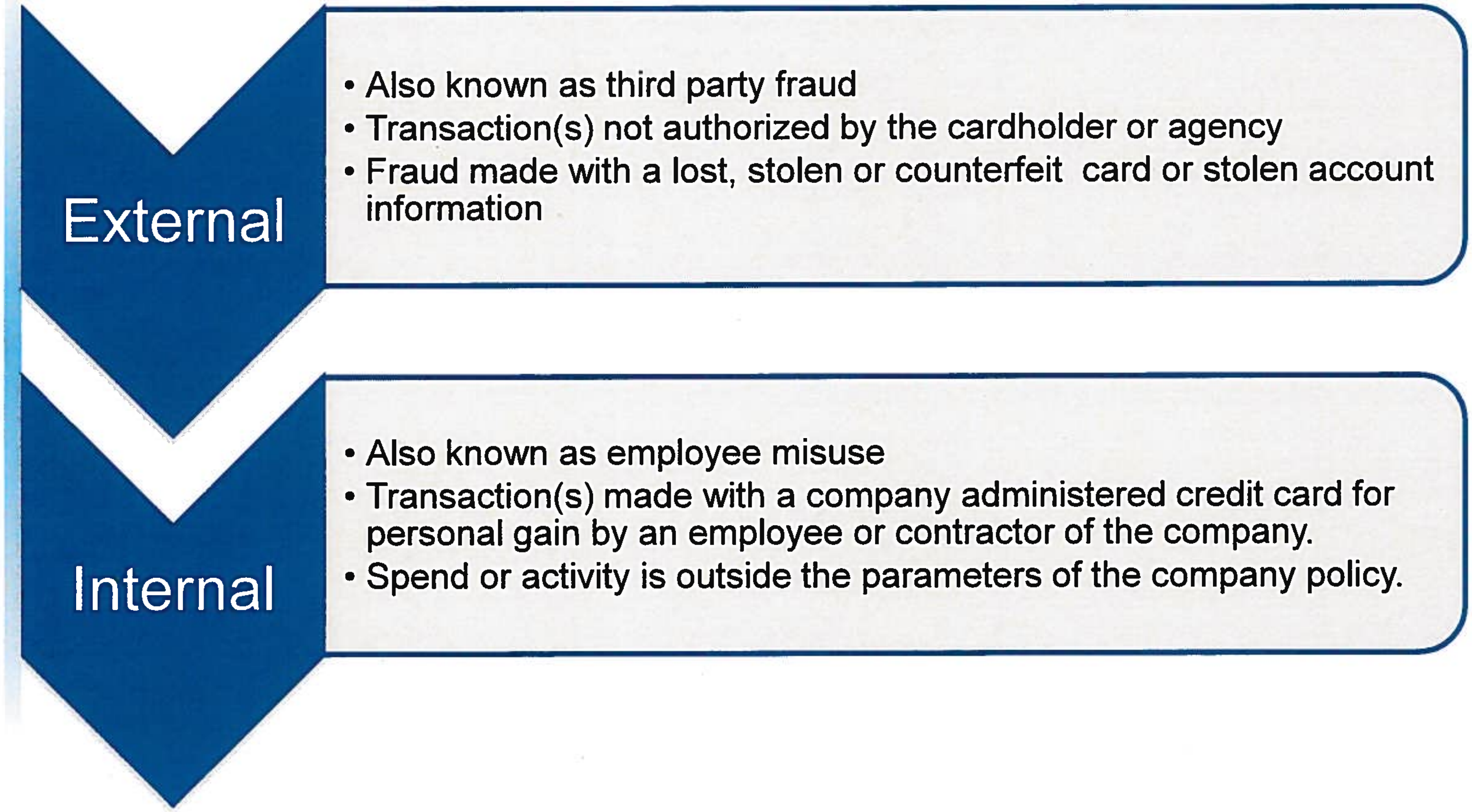
Fraud Prevention Best Practices

John Carr
VP; Card Relationship Manager

What is Fraud?



External

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

Internal

- 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:

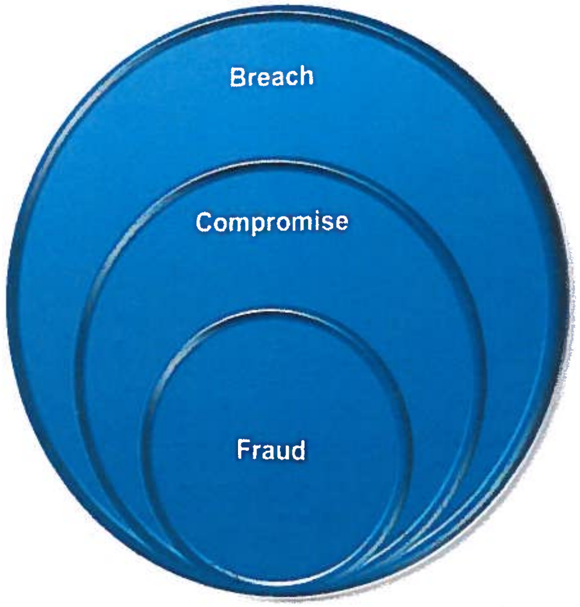
Card Number

Name

Expiration Date

PIN Verification Data: defines and decrypts PIN

Card Verification Value – CVV: unique identifier to specific card



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

Types of Breaches

- **Weaknesses in Merchant/Merchant Processor Network**
  - Merchant networks are accessed using malicious software or some other tool to search for files with credit card data elements (i.e. account number, expiration date, 3 digit card verification value etc.)
  - Access is frequently obtained through a wireless network often at retain type stores
- **Skimming**
  - Device placed on merchant terminal (card reader) that captures magnetic stripe data
  - Most commonly happens at restaurants, ATMs and unattended gas pumps
  - Often cameras are used on conjunction with the skimming device to collect key entered information such as pin number
- **Theft at Merchant**
  - Stolen computer equipment i.e. laptop, thumb drive, etc.
  - Merchant robbed of receipts or records

Types of Breaches

- **Phishing**
  - Perpetrators gain access to critical systems by tricking the merchant or cardholder into providing confidential security credentials, i.e. password, PIN, Card Verification Value (CVV) number etc.
  - Email, phone calls or text messages are the most common methods giving the illusion that the phishing message is coming from a valid source
- **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
  - The process usually begins with a fraudster obtaining one or several valid account number/expiration date pairs

Fraudulent Card Usage

Numerous types of individuals and groups engage in card fraud. These range from individual rookie perpetrators, highly experienced fraudsters, and complex fraud groups/rings. In some instances they work together in partnerships. In most cases there are five key hand-offs that occur between the actual data breach and use of the counterfeit card information in fraudulent transactions:

- **Fraudster steals the raw data** (breach, theft, skimming, etc.)
- **Fraudster sells the data** most commonly via a secured website or on the street. Often the seller will test the data as an extra "service" for the buyer. A test authorization is created on the merchant systems by the fraudster (without the merchants knowledge) to validate the 'good' status of the account information.
- The fraud group/ring **creates counterfeit plastic** by embossing magnetic stripe data on "white plastic", gift cards, or any other card like plastic with a magnetic stripe. This ensures ease/readiness of use.
- Perpetrator and/or the **fraud ring may sell/re-sell** the newly created counterfeit plastic or use themselves.
- A "runner" is often used to take the **merchandise purchased or ATM cash** to another party.

Fraud Department Structure

- Case Analytics and Strategy
- Fraud Detection and Prevention
- Fraud Investigations and Recovery

Fraud Strategy and Case Analytics

- Review fraud cases
- Adjust fraud tools and strategies
- Review false positive fraud ratios
- Participate in industry fraud meetings
- Identify Common Points of Purchase (CPP)
- Work with law enforcement
- Suggest and implement enhancements

Fraud Detection and Prevention

- Analyze accounts
- Contact cardholders to validate transactional activity.
- Work with the Agency Program Coordinators in reaching card members.
- Block accounts, flag fraud transaction(s), fraud report confirmed fraud to Associations.
- Process replacement card requests.
- Initiate recommendations on strategic opportunities related to trends and test merchants.
- Handle inbound calls to verify transaction activity.
- Partner with Agencies on potential misuse situations.

Fraud Detection Systems

- Fraud detection systems are flexible and have the ability to target both general fraud trends as well as specific trends
- Criteria / rules are defined based on analysis of fraud data providing us with current fraud trends
  - Fraud patterns
  - Specific MCC
  - Dollar amounts
  - Geographic location
- Specific merchants
- When authorizations meet these pre-defined criteria, the account is sent to queue or blocked for referral.

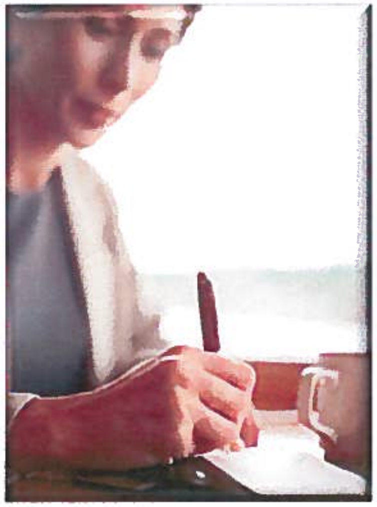
Fraud Investigations and Recovery

- Open fraud cases to maximize recoveries
    - Fraud Report to the Associations
    - Send Affidavit
    - Request and initiate chargeback for recoveries via Association regulations
    - Investigate High Risk Merchant Category Codes to identify potential suspect
    - Analyze for account history for potential point of compromise
    - Work with various law enforcement agencies

- Partner with Program Coordinators on potential misuse in escalating to the Agencies
- Initiate recommendations to Agencies on strategic opportunities related to improved authorization controls

Client Best Practices

- Utilize the card controls available
  - Implement velocity limits on MCCs
  - Review and set credit limits based on usage
  - Limit cash access
  - Review International usage
- Review transaction reports for exceptions and declines
- Educate your cardholders to:
  - Review their transactions and statements
  - Utilize bank owned facilities and ATMs when getting cash
- Use account blocking for temporary leaves or infrequent travelers
- Notification of Voluntary / Involuntary Terminations



Employee Awareness

- Employees should be aware of internal policies about card usage prior to card issuance
  - Consequences of misuse/false fraud reports
  - Importance of immediately reporting a lost or stolen card
  - Limitations on cards- MCCs, velocity limits, cash accessibility
- Other good practices
  - Keep J.P. Morgan's Customer Service telephone number separate from the card in case it is lost or stolen
  - Importance of regular statement reviews
  - ATM usage should be limited to bank owned ATMs
  - Protect pin pad view when entering pin number
  - Awareness of phishing schemes and how to protect their information

Employee Awareness - Phishing

- Phishing is an attempt to gain private information about you and your accounts. Most often via e-mail that looks like it is from your financial institution.
    - It is not JPMorgan's practice to: Send e-mail that requires you to enter personal information directly into the e-mail
    - Send e-mail threatening to close your account if you do not taken immediate action of providing personal information
    - Send e-mail asking you to reply by sending personal information
    - Send e-mail asking you to enter your user ID, password, or account number into an e-mail or non-secure web page
- You should never reply to click on or enter any information if you receive a suspicious e-mail.
- If you are unsure if the e-mail is legitimate call the 800 number on the back of your card

Employee Awareness

- When receiving a phone call from a JPMorgan Commercial Card Representative, it is **not JPMorgan's practice to ask you to provide: Your complete social security number. A representative may ask for the last 4 digits as a verification point**
  - Your card's expiration date
  - CVV or CVV2 from the back of your card
- A Commercial Card Representative may ask you for your account number (usually when returning a message you have left) and **it is our practice to verify at least one piece of personal information.**
- If you are in doubt, do not provide any personal information to the caller and call the 800 number listed on the back of your card to report the incident.