

# CPS Fraud Overview

CPS Fraud Support Analyst

All of **us** serving you®

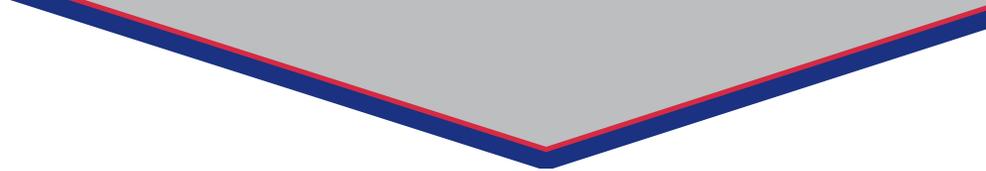


# Agenda

- What is fraud?
- Fraud Trends
- Defending Against Fraud
- Fraud Case Lifecycle
- Tips to Prevent Fraud

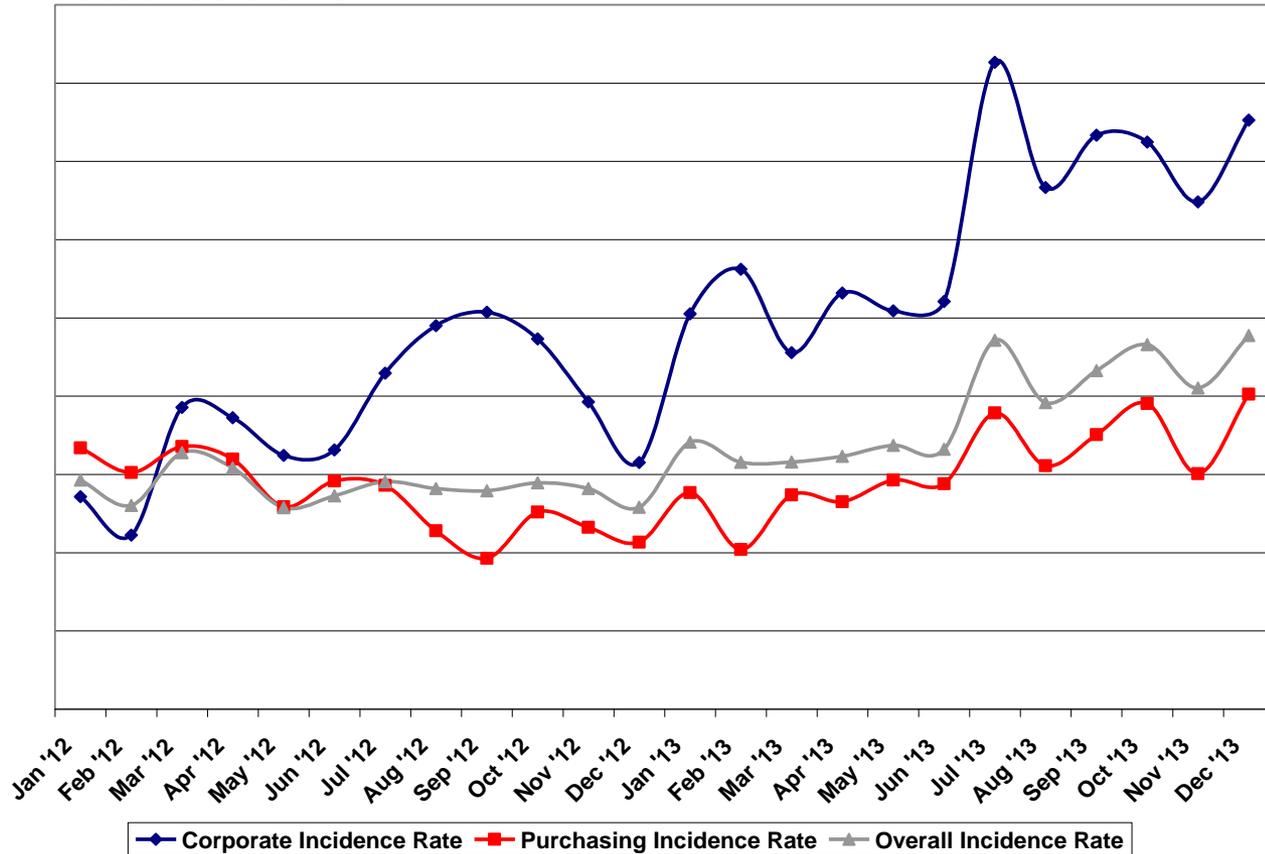
# Defining Card Fraud

- What is Fraud?
  - Unauthorized transactions by an unknown third party
  - Obtaining services, credit or funds by misrepresentation of identity or information
- What is not Fraud?
  - Use by a Friend or Family Member  
*“My 16 year old son took the card from my wallet and spent \$200 at the mall.”*
  - Employee Abuse  
*“A cardholder in my program used their corporate card to pay their utility bill.”*
  - Merchant error/disputed transactions  
*“My purchase was \$42, but the merchant billed me for \$420.”*
  - Inability to pay



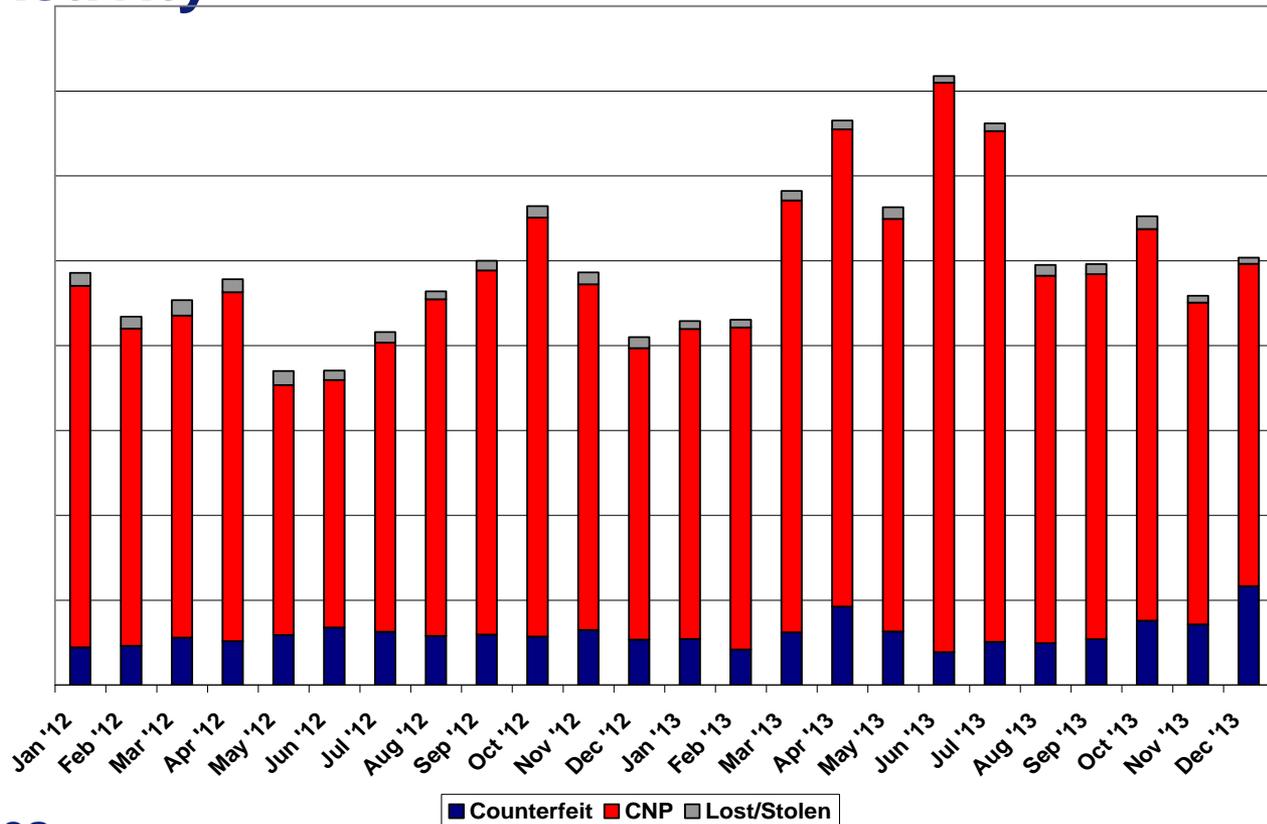
# Fraud Trends

# Fraud Incident Rate



- Incidence rates provide strong indication of overall fraud trend
- The higher the incidence rate, the more fraud we are experiencing
- Compares fraud cases initiated to active accounts

# Fraud Activity



## Fraud Types

- **Counterfeit** – Copy of magnetic stripe captured, also know as card present
- **Internet** – Card number only, also known as card not present (CNP)
- **Lost/Stolen** – Misplaced card or theft

# Most Common Fraud MCCs

Top 10 Fraud by MCC Corp	
MCC	Description
7399	Business Services
7011	Lodging - Hotels, Motels, Resorts
3509	Marriott Hotels
5812	Eating Places, Restaurants
3008	Lufthansa
5399	Misc. General Merchandise
5411	Grocery Stores, Supermarkets
3009	Air Canada
3058	Delta
5732	Electronic Stores

Top 10 Fraud by MCC Purch	
MCC	Description
5999	Miscellaneous & Specialty Retail Stores
5046	Commercial Equipment
5085	Industrial Supplies
5065	Electrical Parts and Equipment
8398	Charitable and Social Service Organizations
5399	Misc. General Merchandise
5732	Electronic Stores
7399	Business Services
5941	Sporting Goods Stores
4215	Courier Services

Top 10 Fraud by MCC Industry	
MCC	Description
5411	Grocery Stores, Supermarkets
5732	Electronic Stores
4722	Travel Agencies & Tour Operators
5542	Automated Fuel Dispenser
5200	Home Supply Warehouse Stores
4511	Airlines, Air Carriers
5311	Department Stores
6012	Financial Institutions – Merchandise/Services
6011	Automated Cash
5310	Discount Stores

- These are only the top 10 most common fraud MCCs
- Evaluate what merchant groups are necessary for your cardholders
- Entire merchant groups can be blocked as needed

# Current Fraud Trends

- Below are the most prevalent trends we are seeing today
  - **Counterfeit/Skimming:** Card's magnetic stripe is copied using a track reading and capturing device
  - **Merchant Compromise:** Interception of magnetic stripe information as it is communicated from merchant to issuer
  - **Identity theft:** Personal information not belonging to the criminal is used to receive financial services
  - **Account number generators:** Method of illegally procuring card information facilitated by the internet

# What are Merchant Compromise Events?

- Merchant systems are hacked
- Issuers detect merchant compromise events through pattern analysis on counterfeit cases
- Card associations are notified of suspected compromises and complete forensic investigations
- U.S. Bank is notified of confirmed merchant compromises by Visa® and/or MasterCard®

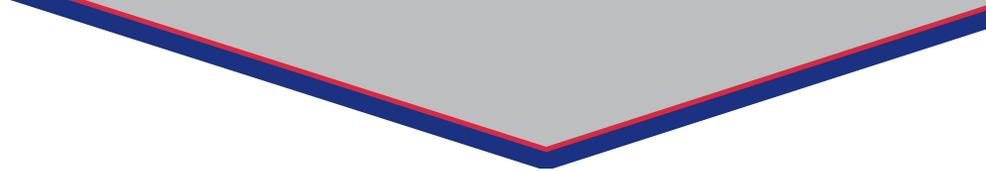
# Account Number Generators (Creditmaster)

```
File Edit Format Help
          CreditMaster v4.0 Copyright 1994 MPI Developm
-----
1/18/02 2:41pm
Extrapolated following 999 cards from 4999 1103 0035 0035:
 1: 4999 1103 0035 0001
 2: 4999 1103 0035 0019
 3: 4999 1103 0035 0027
 4: 4999 1103 0035 0035
 5: 4999 1103 0035 0043
 6: 4999 1103 0035 0050
 7: 4999 1103 0035 0068
 8: 4999 1103 0035 0076
 9: 4999 1103 0035 0084
10: 4999 1103 0035 0092
11: 4999 1103 0035 0100
12: 4999 1103 0035 0118
13: 4999 1103 0035 0126
14: 4999 1103 0035 0134
15: 4999 1103 0035 0142
16: 4999 1103 0035 0159
```

**Numbers Are  
NOT Actual  
Account Numbers**

**A program that generates credit and debit card numbers according to the algorithm used by the major card associations**

- Criminal obtains valid account number
- Programs are only capable of generating account numbers
- All charges are done over the phone or internet (Card Not Present)
- This form of fraud is completely independent of any card activity or usage patterns on the part of the cardholders
- Even cardless accounts can be compromised
- At any given point, Fraud Management is monitoring many active runs



# Defending Against Fraud

# How U.S. Bank Defends Against Fraud

- Develop strategies to decline and/or queue suspicious transactions
  - Monitor for counterfeit test authorizations
  - Watch for increased counterfeit activity by location
- Compare new counterfeit cases against known compromised merchants
  - Assess risk of continued use of compromised card numbers, may suggest a proactive card reissue
- Analyze transaction history of counterfeit cases daily to find new compromise locations

# Analyzing Fraud

- Every morning, the previous day's fraud cases are reviewed for new fraud trends
- As the analytics team identifies new trends they adjust or create strategies to detect and stop these trends
- Strategies are monitored and adjusted daily
- An extensive review of rules is performed monthly to determine areas for improvement and collaborate across U.S. Bank portfolios
- Two types of fraud rules
  - Near-time rules
  - Real-time rules
- Combining real-time strategy with near-time strategy provides us with an effective protection against fraud

## Near-Time Rules

- Fraud system monitors authorizations post-decision and routes highest risk activity including
  - Authorizations over a risk score threshold
  - Authorizations that meet criteria matching current fraud trends
- Fraud detection analysts review the accounts in queue
  - Add or remove the Referral Block (FR)
  - Call cardholder to confirm activity, leave block in place if unable to reach cardholder

## Real-Time Rules

- A real-time rule declines or refers at the point of sale
- Reserved for activity with the highest fraud risk
- Decline reason is 'ADS I Strategy/ADS II FILTER' which stands for Authorization Decision Strategy



# Fraud Case Lifecycle

# What Happens if Fraud is Confirmed?

- Fraud claim is initiated
- Card will be closed as a result of claim initiation
- Notations added to the account memo
- Case submitted in fraud system
- Any follow-up questions are directed to FDSS (Fraud and Disputes Solution Services team)

# Fraud Case Process

- Fraud cases should be initiated over the phone. Please do not use mail, fax or online processes to initiate fraud
- Contact Cardmember Service at 800-344-5696 (Corporate) or 888-994-6722 (Government)
- The Service Advisor transfers the customer to our fraud department (800-523-9078) where they will review the current activity with the cardholder
- The Fraud Representative will initiate the case by marking the authorizations and/or transactions that have posted to the account that are believed to be fraudulent
  - Because a third party has gained access to your account information we will ask you to close your account as we are required to do so. It will be replaced with a new number and all account information transferred
- Changes to the fraud card are processed including credit rating, address, company number and agent number
- Case Processor is assigned to monitor the account to see if charges have posted
- If the fraud charges post to your new account you will receive a credit to your account and sent a statement of fraud to confirm that you did not authorize those transactions

# Fraud Case Process Cont'd

- The statement of fraud form will be generated based on the posted fraud transactions and mailed within 3 weeks of case initiation. If the case is started on authorization activity and the transactions never post, no statement of fraud will be created and the case will be closed
  - The statement of fraud will be mailed to the system address on the card. If there is a request to fax or mail to an alternate address please call the Fraud Department to request these changes
- The statement of fraud will need to be completed by the cardholder and returned to the Fraud Department by the due date on the form
- Once the statement of fraud is received an investigation will be conducted to determine who is responsible for the fraud
  - If it is discovered that the cardholder participated or benefited from the charges the account will be re-billed and the claim denied
  - If the claim is resolved in the cardholder's favor the credit will remain on the account permanently
- If the signed statement of fraud is not received by the bank, the new account will have the charges reapplied and the cardholder will be liable to pay for them



# Tips to Prevent Fraud

# Program Administrator Tips

- Review spending reports and question non-business related transactions
  - **Suspend or cancel charging privileges when appropriate**
- Be mindful of how card data is stored and destroyed
- Keep cardholder account records current
- Ensure that termination includes destroying the card and closing the account
- Notify Account Coordinator of anticipated changes in spending patterns
- Frequently communicate policies on appropriate use of the card and how to report suspicious activity
- Schedule fraud reports to monitor activity and ensure the statement of fraud affidavit is returned to the bank. They can be scheduled to go to your Access Online Data Exchange mailbox
  - **Statement of Fraud Report** includes all fraud cases that were opened in the past 90 days and show when the document was sent and if/when it was received back by U.S. Bank
  - **Fraud Summary Report** includes all authorizations and transactions identified as fraud for each fraud case during the time frame requested. The report also summarizes the top fraud MCCs by count and dollar amount

# Cardholder Tips

- Sign your cards as soon as they arrive
- Don't lend your card or personal identification number (PIN) to anyone
- Don't leave cards or receipts lying around
- Keep an eye on your card during the transaction and get it back as quickly as possible
- Destroy receipts and statements you no longer need
- Reconcile accounts frequently
- Report any questionable charges promptly to U.S. Bank
- Notify card companies in advance of a change in address or phone number
- Don't write your account number or personal information down
- Don't give out personal information over the phone unless you initiated the call and the company is reputable
- Keep a record of your account numbers, their expiration dates, and the phone number and address of each issuer in a secure place