



A
Winning
HAND:

**Civilian Agency Elective: External Fraud
Trends and Mitigation Practices (Non-DoD)**

Deanna Hanson
CPS Fraud Support Analyst

Agenda

- What is fraud?
- Fraud trends
- Fraud case lifecycle
- Fraud and dispute process
- Tips to prevent fraud



Defining Card Fraud

- What is card fraud?
 - Obtaining services, credit or funds by misrepresentation of identity or information
 - Third-party, unauthorized use of a card



Defining Fraud

- Fraud is defined as third-party unauthorized use of a card. Common fraud situations include:
 - Swiped transactions after the card is lost or stolen
 - Internet charges at sites where the cardholder has not made a purchase or waiting for an order
 - A swiped transaction appearing out of the cardholder's home area and the cardholder still has their card (counterfeiting)



Fraud is not...

- Cardholder / employee abuse
- Family use
- Marital situations
- Misuse and abuse
- Disputed transactions / charge error
- Inability to pay

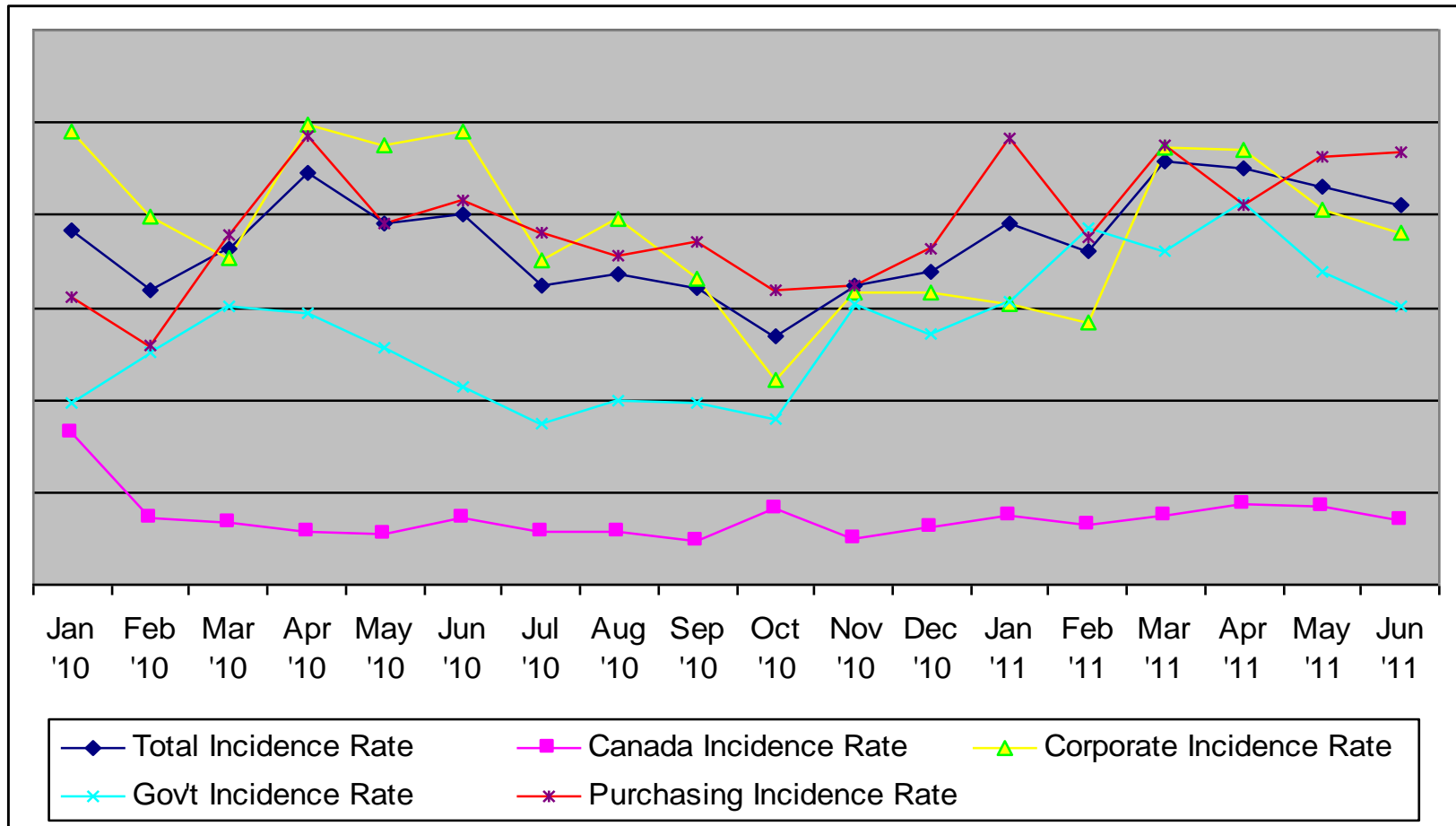


Fraud Trends

All of **us** serving you®



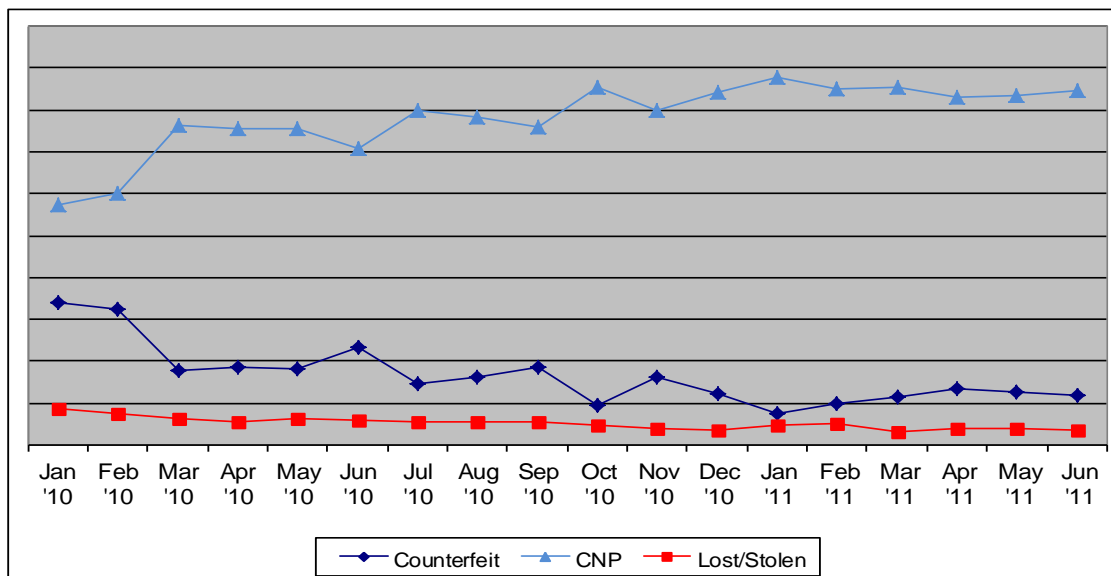
Fraud Incident Rate



Fraud Activity

Fraud Types

- **Counterfeit** – Copy of magnetic stripe, perpetrated by organized criminal groups
- **Internet / Card Not Present (CNP)** – Unauthorized use of account information, card number only
- **Lost / Stolen** – Crimes of convenience
- **Non-Receipt of Issued card (NRI) / mail theft** – Minimal risk if issuer uses a card activation program
- **Account Take Over (ATO)** – Identity theft is not an issue for our travel and purchasing card portfolios



Most Common Fraud Locations

Top 10 Fraud MCCs in Q1/Q2 for GSA Travel & Fleet Cards

GSA Travel & Fleet - Q1		
Merchant Category	Description	% of Total
5411	Grocery Stores & Supermarkets	15.6%
7399	Business Services not elsewhere classified	10.2%
5542	Automated Fuel Dispenser	8.1%
7011	Lodging - Hotels, Motels & Resorts	6.3%
3058	Delta	5.9%
3512	Intercontinental	4.6%
3703	Residence Inn	4.2%
3722	Wyndham	3.9%
3692	Doubletree	3.5%
3501	Holiday Inns	2.9%

GSA Travel & Fleet- Q2		
Merchant Category	Description	% of Total
5411	Grocery Stores & Supermarkets	23.9%
5542	Automated Fuel Dispenser	14.0%
3504	Hilton	10.8%
6011	Financial Institutions - Automated Cash Disbursements	5.9%
3750	Crowne Plaza Hotels	5.3%
7011	Lodging - Hotels, Motels & Resorts	4.7%
5912	Drug Store & Pharmacies	3.7%
5541	Service Stations	3.7%
3501	Holiday Inns	2.6%
3509	Marriott	2.4%



Most Common Fraud Locations

Top 10 Fraud MCCs in Q1/Q2 for GSA Purchasing Cards

GSA Purchasing - Q1		
Merchant Category	Description	% of Total
5047	Dental/Laboratory/Medical/Ophthalmic Hosp Equip & Sup	19.3%
7699	Miscellaneous Repair Shops & Related Services	9.0%
8220	Colleges, Universities, schools	8.5%
5533	Automotive Parts & Accessories	3.0%
5940	Bicycle Shops	2.8%
5571	Motorcycle Dealers	2.8%
5999	Miscellaneous & Specialty Retail	2.2%
5200	Home Supply Warehouse Stores	2.1%
8398	Charitable & Social Service Organizations	1.9%
5085	Industrial Supplies	1.7%

GSA Purchasing - Q2		
Merchant Category	Description	% of Total
5047	Dental/Laboratory/Medical Sup	14.6%
5045	Computers and equipment	5.2%
5940	Bicycle Shops	4.5%
5999	Miscellaneous & Specialty Retail	3.8%
5969	Direct Marketing	3.3%
5964	Catalog Merchants	3.1%
5085	Industrial Supplies	2.9%
8398	Charitable & Social Service Organizations	2.7%
7399	Business Services	2.5%
5691	Men's & Women's Clothing Stores	2.3%



Current Fraud Trends

- Organized crime drives each of these trends
 - **Skimming:** Card's magnetic stripe is copied using a track reading and capturing device
 - **Data breach events:** Intentional 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. Victim is left with the responsibility of cleaning up his/her credit bureau and the associated negative impacts
 - **Account number generators:** Method of illegally procuring and using card information facilitated by the Internet
- U.S. Bank clients rarely notify us of identity theft, however the other three trends impact us regularly



Counterfeit Fraud – What are Data Breach Events

- Merchant systems are hacked or “sniffed”
- Issuers detect data breach events through pattern analysis on counterfeit cases
- Card associations are notified of suspected breaches
- Card associations complete forensic investigations
- U.S. Bank is notified of confirmed data breaches by Visa[®] and/or MasterCard[®]
 - Both Visa and MasterCard follow specific procedures before notifying issuers, thus the increased time for identification



U.S. Bank Defends Against Counterfeit Fraud

- Develop strategies to decline and/or queue suspicious transactions
 - Counterfeit test authorization merchants
 - Increase in counterfeit activity at a specific 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 histories of counterfeit cases to find new compromise location



Account Number Generators - Creditmaster

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

- Criminal obtains valid account number and expiration date
- Even cardless accounts can be compromised
- At any given point, Fraud Management is monitoring many active runs
- All charges are done over the phone or internet – Card Not Present

```
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**

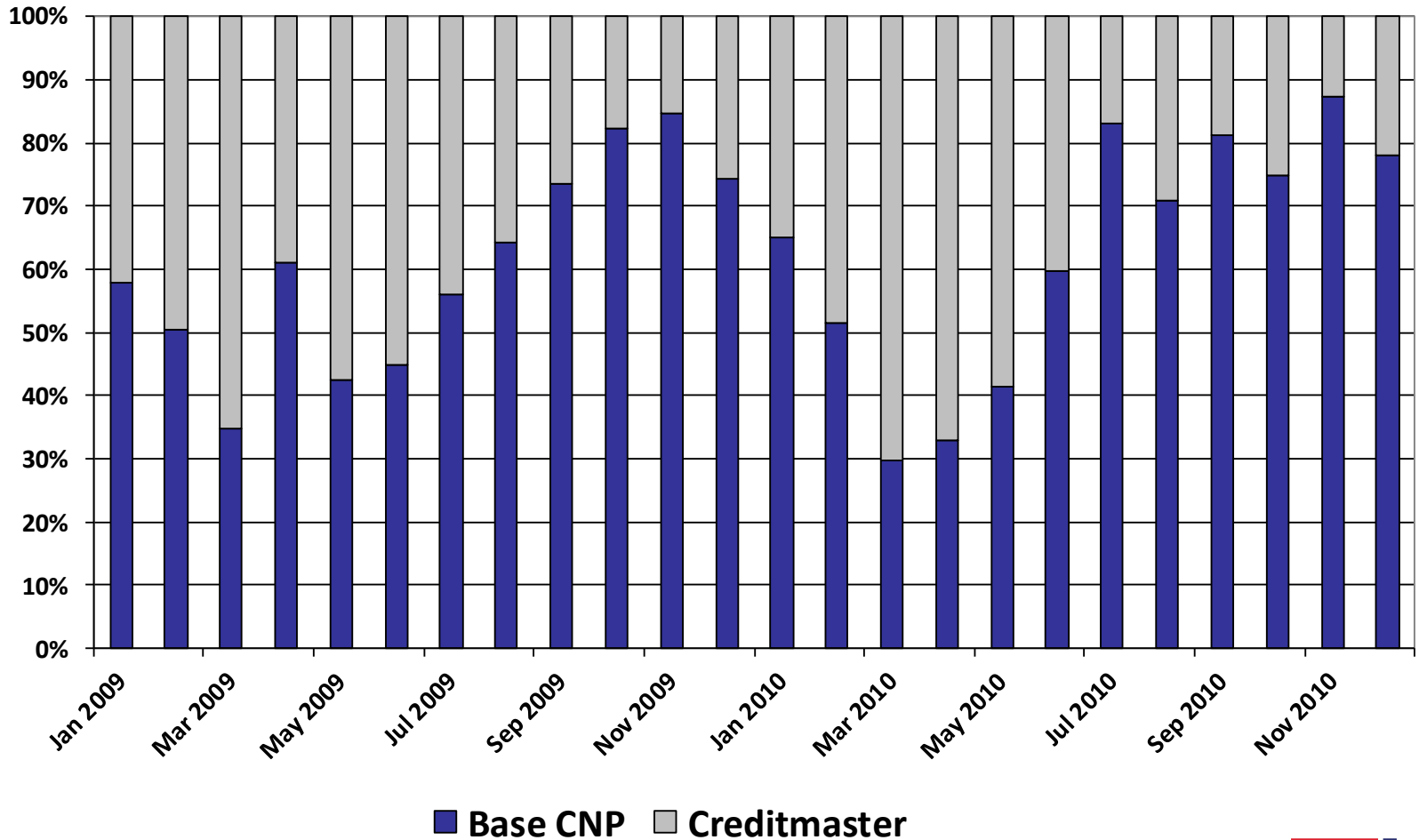


Account Number Generators

- Important points to remember
 - This form of fraud is completely independent of any card activity or usage patterns on the part of the cardholders
 - Programs are only capable of generating numbers
- How does U.S. Bank defend against account number generators?
 - Create rules to send accounts to a detection queue
 - Decline fraud transaction pattern at the point of sale



Card Not Present Fraud



Fraud Case Life Cycle

All of **us** serving you®



Analyzing Fraud

- Every morning the previous days 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
- Rules are monitored and adjusted daily
- Two types of fraud rules
 - Near-time rules
 - Real-time rules



Near-Time Rules

- Fraud system monitors authorizations post-decision and routes highest risk activity
 - Authorizations over a risk score threshold
 - Authorizations that meet criteria matching current fraud trends
- Fraud detection analysts review the accounts in queue
 - Add and/or remove the Referral Block (FR)
 - Call cardholder, 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 which stands for Authorization Decision Strategy



Fraud Protection Tool Summary

- Combining real-time strategy with near-time strategy in the system provides us with an effective protection system against fraud
 - Real-time declines are designed to potentially block fraud on the first detected attempt
 - Near-time alerts then provide an opportunity to block subsequent fraud attempts
- Rules are monitored regularly to ensure they are performing as designed
 - Rules are updated or deleted as needed



What Happens if Fraud is Confirmed?

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



Working the Fraud Case

- The case appears in a case processing queue the following day
- Report runs which assists in changes to the fraud card
- Case Processor is assigned who monitors the account to see if charges have posted
- If all fraud charges have posted the statement of fraud is generated, if there are outstanding authorizations the case is pended to allow those transactions to post
- Only one statement of fraud will be sent out on an account, based on the transactions identified as fraud when the account was closed and the case was started
- The statement of fraud must be signed and returned by the cardholder by the due date on the form



Tips to Mitigate and Detect Fraud

All of **us** serving you®



Program Administrator Tips

- Review spending reports & question non-business related transactions immediately
 - Suspend or cancel charging privileges when appropriate
- Be mindful of how card data is stored and destroyed
 - Card associations have stringent regulations for merchants around the storage of card account or transaction data
- Keep cardholder account records current
 - Assist cardholders in providing issuers with up to date contact information via regular file updates to U.S. Bank
- 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 account and how to report suspicious activity



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 on a postcard or the outside of an envelope
- 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





Questions?



Thank You

Presentations will be available on
www.usbank.com/sp2presentations
after the conference

©2011 U.S. Bank National Association. U.S. Bank Government Services is a division of U.S. Bank National Association ND. All other trademarks are the property of their respective owners. This publication is neither paid for, sponsored by, nor implies endorsement, in whole or in part, by any element of the United States Government. The information provided is for general use only. Contact the GSA Contracting Office with any questions related to proper use of the master contract. Printed in the USA.

