USDA: Handling Fraud and Disputes

Deanna Hanson
CPS Fraud Support Analyst

All of us serving you®

usbank®

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

Fraud is Not…

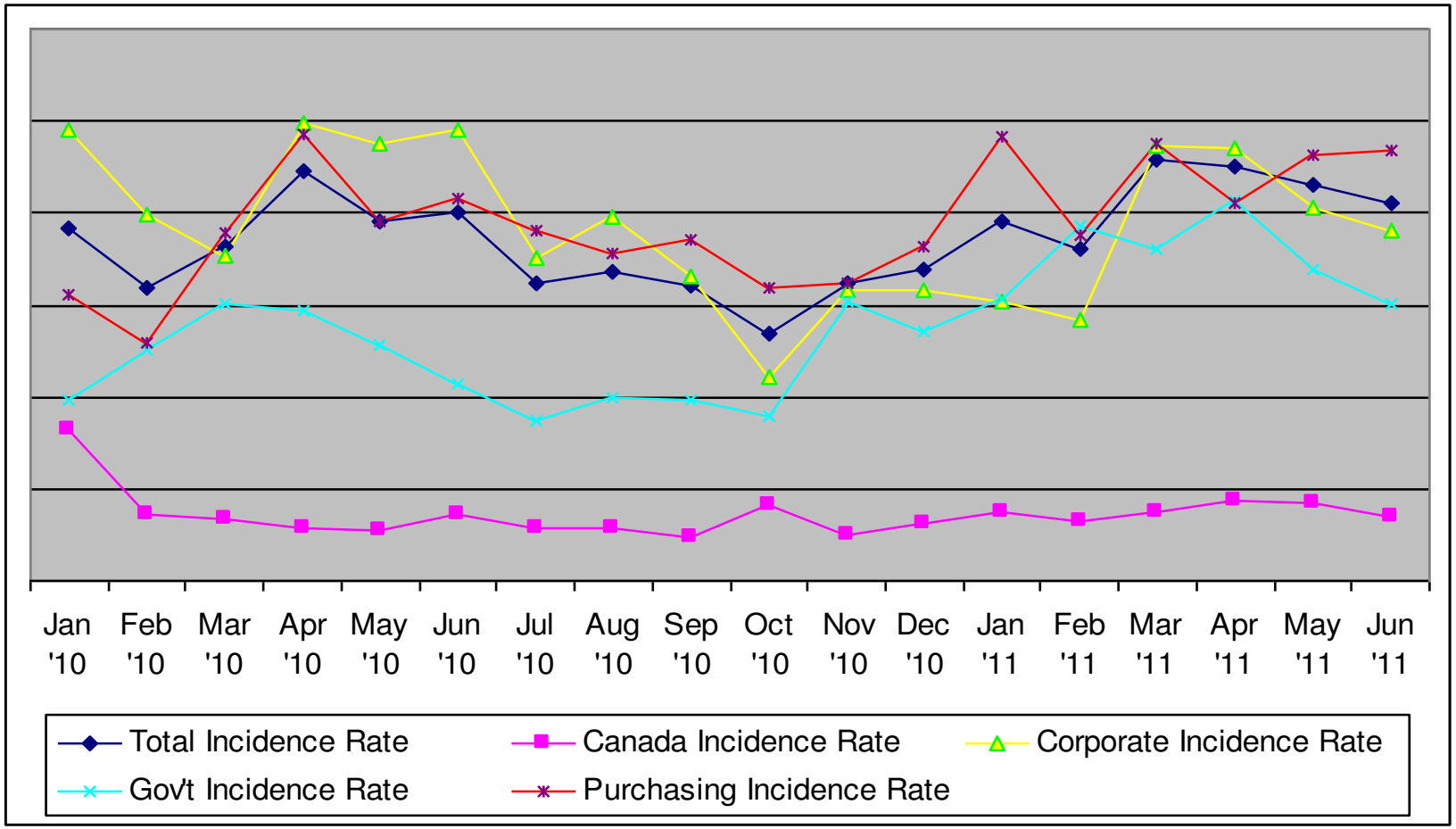
- Cardholder / employee abuse
- Family use
- Marital situations
- Misuse and abuse
- Disputed transactions/charge error
- Inability to pay

Fraud Trends

All of us serving you®

usbank®

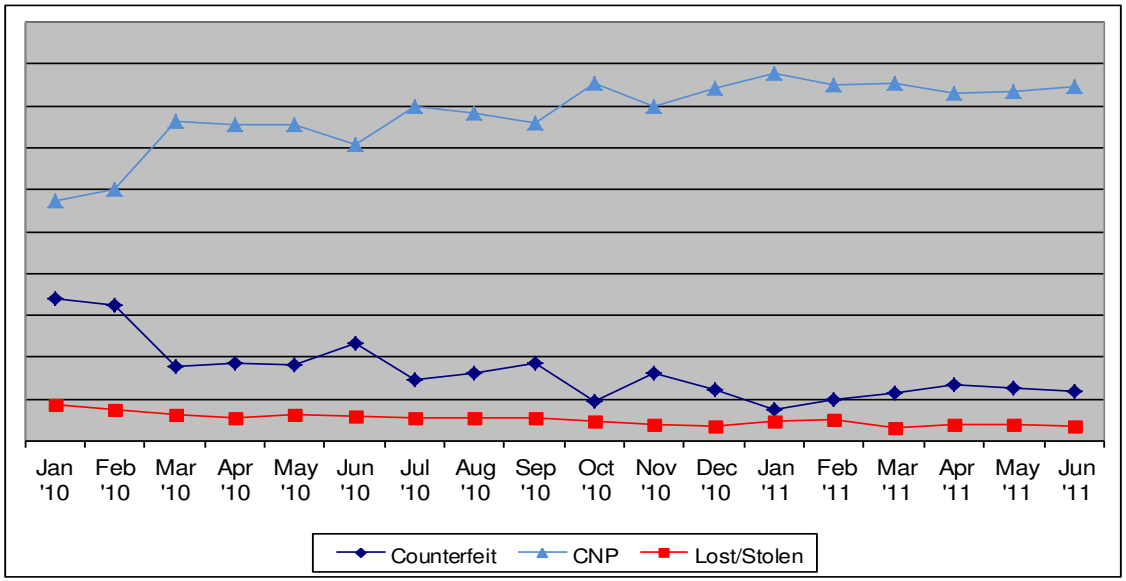
Fraud Incident Rate



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

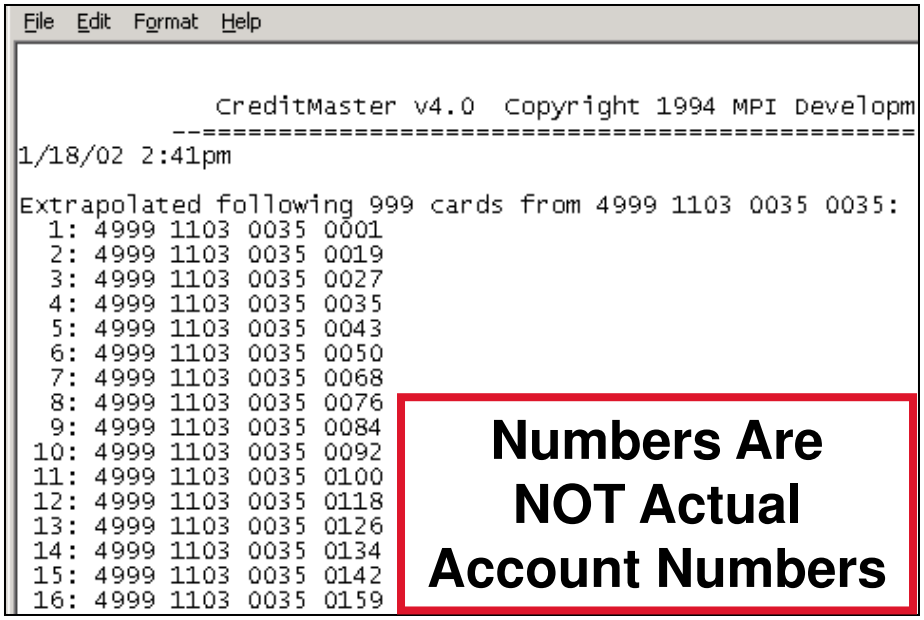
U.S. Bank Defends Against Counterfeit Fraud

- 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

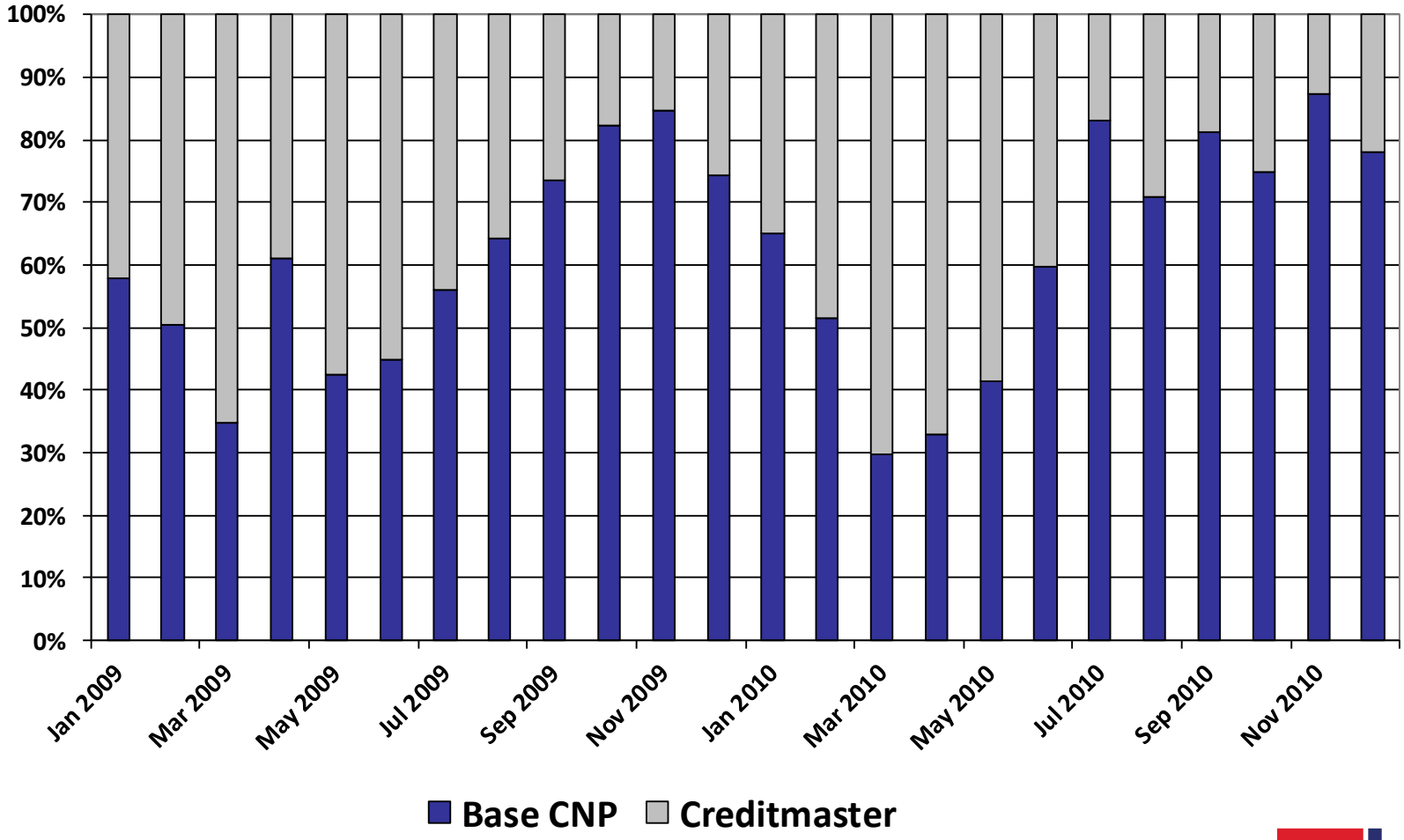
- Criminal obtains valid account number and expiration date
- Even cardless accounts can be compromised
- At any given point, Fraud Management is monitoring many active runs
- All charges are done over the phone or internet – Card Not Present



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®

usbank®

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
- 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 Fraud 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”

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

Complete Fraud and Dispute Process

Client document available upon request from your Relationship Management team

All of us serving you®

usbank®

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)

Items to Remember With Fraud

- Fraud cases should be initiated over the phone.
- You will be asked to close your card. We will replace it with a new number.
- If the fraud charges post to your new number you will receive a credit to your new account and will be sent a Statement of Fraud to confirm that you did not authorize those transactions.
- The Statement of Fraud will need to be completed and returned to the Fraud Department by the due date on the letter.
  - If the signed Statement of Fraud is not received by U.S. Bank, the new account will have the charges reapplied and the cardholder will be liable to pay for them.

Reporting Fraud

- Contact Government Services at 888-994-6722. Your account will be closed, transferred to a new number and a new card will be issued:
  - The Service Advisor transfers the customer to our fraud department (800-523-9078) where they will review the current activity on the account 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 transactions.
  - A Statement of Fraud form will be generated based on the posted fraud transactions and mailed out within 3 weeks of the call. If the case is started on authorization activity and the transactions never post, a Statement of Fraud letter will not be created and the case will be closed.

What if I have a Question Regarding Fraud?

- Questions on initiating a fraud case:
  - Contact Government Services at 888-994-6722. They will ask you questions and then transfer you to our fraud department. Both departments are available 24 hours a day, 7 days a week.
- Questions on existing fraud cases:
  - Contact U.S. Bank's FDSS Team at 800-815-1405
  - If assigned to a case processor you may contact them directly at their extension
  - You may also call Government Services, using the number on the back of your card. They will connect you with the appropriate fraud representative.

Defining Dispute Cases

- Dispute situations are defined as a disagreement between the merchant and the cardholder where the cardholder is asking for their Issuer's assistance. Visa and MasterCard regulations offer assistance with a variety of dispute reasons. Some of the more common reasons are:
  - Merchandise or service not received
  - Merchandise returned
  - Duplicate processing
  - Unrecognized
  - There are additional dispute types not listed above
- Please contact Government Services for more information on specific scenarios.

Instructions for Disputing a Sales Transaction

- Before disputing or questioning a charge on the statement, please validate that you have taken the following actions:
  - Review receipts for the amount in question as it may have posted to the statement with a different merchant name or with a different amount
  - Attempt to contact the merchant to resolve the issue

If neither you nor anyone authorized to use the card recognize the transaction as one you participated in, please call Government Services 24/7 at 888-994-6722, where they will assess the proper action to be taken including initiating a dispute or fraud case. (See above: Reporting Fraud)

Initiating a Dispute Case

- If you still desire to dispute the transaction after attempting to contact the merchant and verifying your receipts, chose one of the following options to initiate a case:
  - Fill out the dispute interview on U.S. Bank Access® Online explaining the reason for filing the dispute and the transaction information
  - Phone by calling Government Services at 888-994-6722
  - Send it in writing via fax or mail using the Cardholder Statement of Questioned Item form (CSQI)
    - Include a detailed letter explaining the reason for filing the dispute and the transaction information. Sent the form to:

      Dispute Department

      PO Box 6335
      Fargo ND 58125-6335

      Fax: 866-229-9625
      Attn: Dispute Department

Important Information to Include When Initiating a Billing Dispute Case

- When initiating a dispute it is important that the following information be provided to U.S. Bank:
  - The account number information and details on the transaction in question (date and dollar amount)
  - Your contact information including a daytime phone number, including area code
  - An explanation of why you believe there is an error or why you need additional information
  - Any supporting documentation
  - The date you contacted the merchant and details

Time Frames for Dispute Cases

- All billing dispute cases need to be initiated within 90 days from date the transaction posted to the account
- If you wish to initiate a case that is beyond the 90 day timeframe you may still attempt the case by calling Government Services, by mailing in a letter, or by faxing a letter to the contact information listed above

What Will Happen After the Case is Started?

- Once the request to initiate a dispute is received by U.S. Bank a variety of steps will occur:
  - The amount of the transaction will be suspended.
  - You will receive communications regarding the status of your claim and requests for additional information. Many of these letters are time sensitive and require a cardholder response.
  - Since disputes are governed by Visa and MasterCard Regulations, all disputes require that certain criteria must be met in order to pursue dispute rights.

What Will Happen After the Case is Started? (Continued)

- If all requirements are met, U.S. Bank will attempt to return the charge (chargeback) to the merchant. If this occurs you will receive a provisional credit for the disputed amount on your account and the suspension will be lifted.
- The merchant has an opportunity to respond (represent) through Visa and MasterCard. If this happens you maybe required to provide an updated response to the merchant's rebuttal.
- You will be notified if additional information is needed.
- If the claim is resolved in your favor your provisional credit will remain on the account as a permanent credit. If the claim is not resolved in your favor the charge will be reposted to the account.
  - Dispute cases may be very complex and are not guaranteed to be successful. U.S. Bank is required to follow Visa and MasterCard regulations for disputes.

What if I Have Questions?

- Initiating a dispute case:
  - Contact Government Services at 888-994-6722
- Existing dispute case:
  - Contact U.S. Bank's FDSS Team at 800-815-1405 (This number is for existing Fraud or Dispute cases only)
  - If assigned to a Case Processor you may contact them directly at their extension
  - You may also call Government Services, using the number on the back of your card. They will connect you with the appropriate dispute representative

Tips to Mitigate and Detect Fraud

Client document available upon request from your Relationship Management team

All of us serving you®

usbank®

Program Administrator Tips

- Review spending reports and 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 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