

Fraud, Delinquency and Dispute Management (Non-DoD)

Deanna Hanson and Todd Bishop

All of **us** serving you®



Agenda

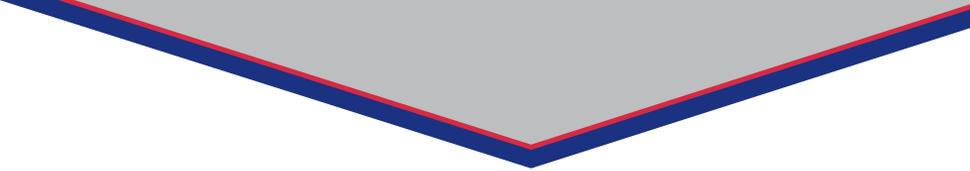
- Fraud Management
 - What is fraud?
 - Fraud trends
 - Fraud case lifecycle
 - Tips to prevent fraud

Agenda (Continued)

- Delinquency Management
 - Best practices – Credit risk management
 - Creditworthiness review
 - Account suspension guidelines
 - Collections strategies
- Dispute Management
 - Dispute definition and cardholder requirements
 - Valid / invalid disputes
 - Dispute timeframes
 - Dispute process
- Questions and answers

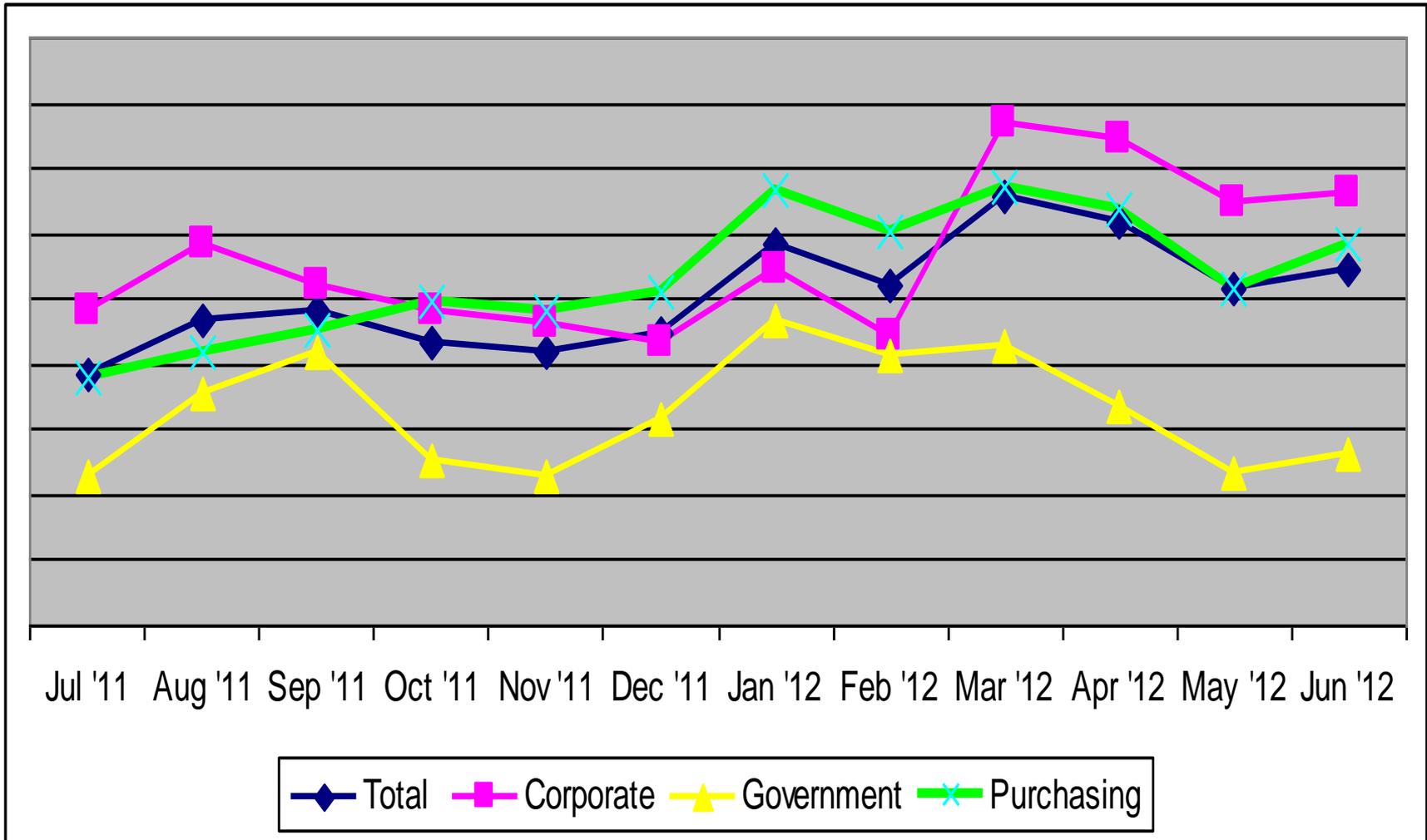
Defining Card Fraud

- 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
 - Misuse and abuse
 - Disputed transactions/charge error
 - Inability to pay



Fraud Trends

Fraud Incident Rate

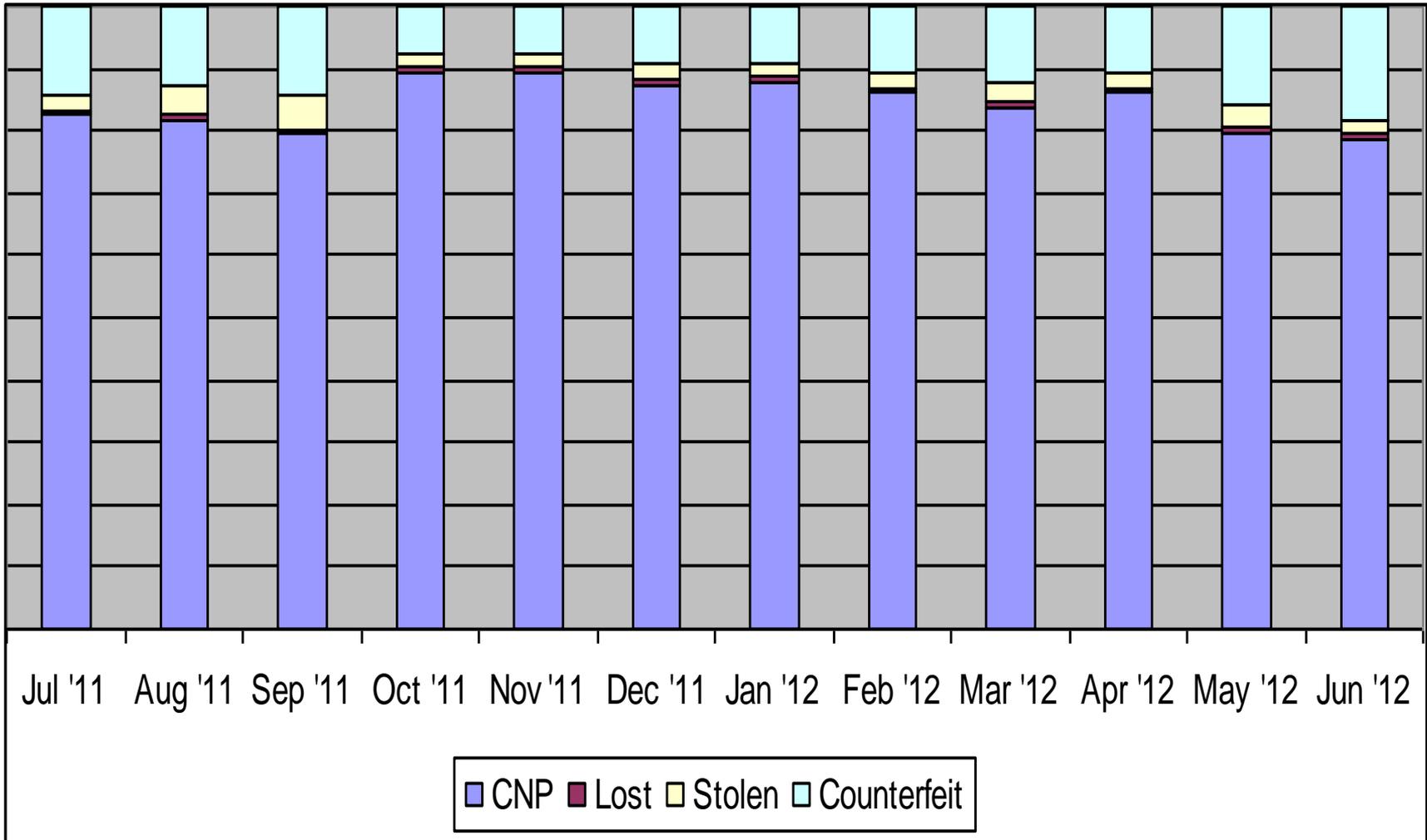


Fraud Activity

- Fraud Types

- **Counterfeit:** Copy of magnetic stripe, perpetrated by organized criminal group
- **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

Fraud Activity Rates



Most Common Fraud Locations

Top 10 Fraud Merchant Category Codes (MCCs) Q1 - Q2 for Purchasing Cards

GSA Purchasing Top Fraud MCCs		
MCC	Description	% of Fraud
5047	Dental/Lab/Medical Equip	15.9%
5045	Computers, Equipment, Software	5.4%
7399	Business Services	3.8%
5085	Industrial Supplies	3.2%
5941	Sporting Goods Stores	2.9%
5999	Misc & Specialty Retail Stores	2.9%
5964	Catalog Merchant	2.9%
9399	Government Services	2.9%
5251	Hardware Stores	2.6%
5732	Electronics Stores	2.3%

Most Common Fraud Locations

Top 10 Fraud MCCs Q1 – Q2 for Travel Cards

GSA Travel Top Fraud MCCs		
MCC	Description	% of Fraud
5411	Grocery & Supermarkets	14.8%
5944	Jewelry, watch, clock & silverware	6.6%
5310	Discount Stores	5.2%
5542	Automated Fuel Dispenser	3.8%
6011	Automated Cash Disbursement	3.7%
4812	Telecommunication Equip & Sales	3.3%
3701	La Mansion Del Rio	3.1%
7011	Lodging	2.8%
3665	Hampton Inns	2.6%
5732	Electronics Stores	2.6%

Current Fraud Trends

- Trends driven by organized crime
 - **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
 - **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 – Data Breach Events

- Merchant systems are hacked or “sniffed”
- Issuers detect data breach events through pattern analysis on counterfeit cases
- Card payment networks are notified of suspected breaches
- Card payment networks 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

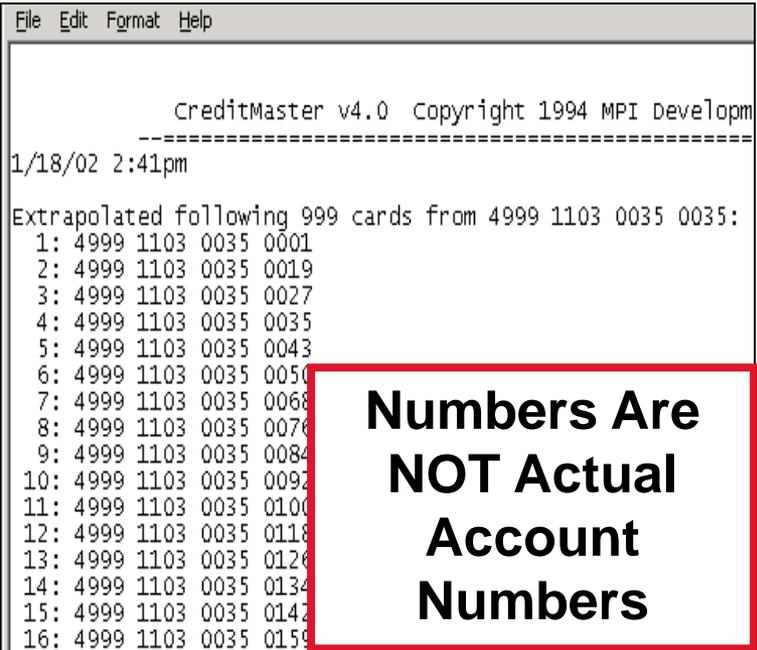
Defenses Against Counterfeit Fraud

- Develop strategies to decline and/or queue suspicious transactions which include
 - 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 payment networks

- 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 transactions

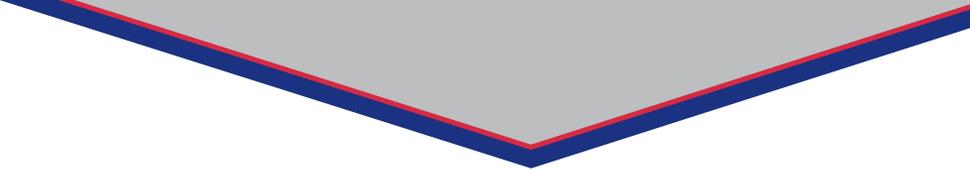


```
File Edit Format Help
          CreditMaster v4.0 Copyright 1994 MPI Developm
-----
1/18/02 2:41pm
Extrapolated following 999 cards from 4999 1103 0035 0035:
 1: 4999 1103 0035 0001
 2: 4999 1103 0035 0019
 3: 4999 1103 0035 0027
 4: 4999 1103 0035 0035
 5: 4999 1103 0035 0043
 6: 4999 1103 0035 0051
 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 0150
```

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?
 - Monitor fraud activity trends
 - Create rules to send accounts to a detection queue
 - Decline fraud transaction pattern at the point-of-sale



Fraud Case Life Cycle

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 prevent 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, it routes highest risk activity and may systematically place a Fraud Referral (FR) code on the account
 - Authorizations which exceed a risk score threshold or meet criteria matching current fraud trend
- Fraud detection analysts review the accounts in queue
 - Add and/or remove the FR block
 - 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 1” (Authorization Decision Strategy)

Fraud Protection Tool Summary

- Combining real-time strategy with near-time strategy in the system results in an effective protection system against fraud
 - Real-time strategies are designed to potentially block fraud on the first detected attempt
 - Near-time strategies 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

Reporting Fraud

- Fraud cases should be initiated over the phone by contacting Government Services at 888-994-6722 immediately
- Customer will be asked to close the account. A replacement account will be reissued
- Customer will be transferred to our Fraud Department (800-523-9078), who will review the current activity with the cardholder
- Fraud analyst will initiate a fraud case by identifying the authorizations and/or transactions that have posted to the account that are believed to be fraudulent transactions

Reporting Fraud (continued)

- If the fraud charges post to the customer's new account, they will receive a credit on the new account
- A Statement of Fraud form will be sent to the cardholder
- 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
- The Statement of Fraud must be completed and returned to the Fraud Department by the due date on the letter

Reporting Fraud

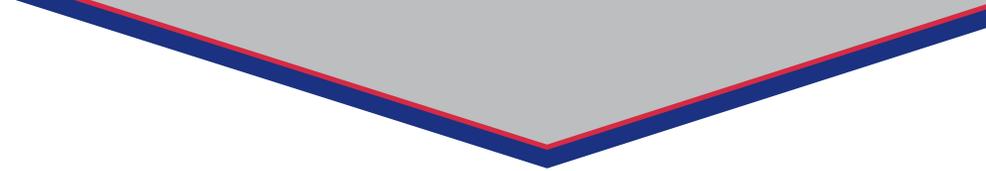
- If the fraud charges post to the customer's new account, they will receive a credit on the new account
- A Statement of Fraud form will be sent to the cardholder
- If the case is started on authorization activity and the transactions never post, a Statement of Fraud letter will not be created and the case will be closed
- The Statement of Fraud must be completed and returned to the Fraud Department by the due date on the letter

Contact Information

- Questions on existing fraud cases:
 - Contact the U.S. Bank Fraud & Disputes Solutions Service (FDSS) at 800-815-1405, available 24/7
 - If a case is assigned to a case processor, the cardholder may contact them directly at their extension
 - Contact Government Services at 888-994-6722, available 24/7

Time Frames for Fraud Cases

- All fraud cases need to be initiated within 90 days of the transaction posting date, however the sooner the better
- The Statement of Fraud will be sent within three weeks of the case being initiated
- The signed Statement of Fraud must be returned within 21 days from the date it was generated
- If the case is not started and/or the Statement of Fraud is not returned within these dates, the client will be liable for the transactions



Tips to Mitigate and Detect Fraud

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
- 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 account and how to report suspicious activity

Program Administrator Tips (Continued)

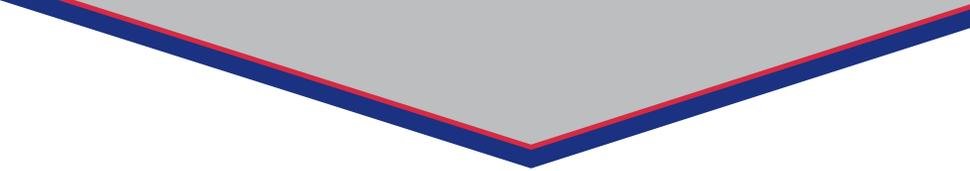
- Schedule fraud reports to monitor activity and ensure the Statement of Fraud Affidavit is returned to the bank. They can be scheduled to go to your Access Online Data Exchange mailbox
 - **Statement of Fraud Report** includes all fraud cases that were opened in the past 90 days and show when the document 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 of the fraud cases 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 to U.S. Bank promptly

Cardholder Tips (Continued)

- Notify U.S. Bank 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, same for emails or internet activity
- Keep a record of your account numbers, their expiration dates, and the phone number and address of each issuer in a secure place



Delinquency & Credit Risk Management

Best Practices – Credit Risk Management

- Participate in Creditworthiness
 - Assign limits and card access based on cardholder risk
 - Credit scores predict risk
 - Actively assign limits based on anticipated cardholder travel needs, not on default limits
 - Update account scores quarterly and adjust limits/card access based on most recent risk assessment

Best Practices – Credit Risk Management

- Monitor and review Delinquency Reports
 - Route to department managers for one-to-one discussions with cardholders
 - Immediately address accounts that default on first payment
 - Address all accounts with a payment returned for non-sufficient funds (NSF)
 - Accounts with 2 NSF payments within 12 months should be cancelled
 - Close accounts that have been 90 days past due twice within last 12 months AND are presently 60 days past due

Best Practices – Credit Risk Management (Continued)

- Monitor cash usage
 - Address accounts with multiple cash advances near their billing address
- Mandate salary offset
- Work with your U.S. Bank Relationship Manager to improve agency rebates by addressing ways to:
 - Improve file turn
 - Control delinquencies
 - Limit and reduce losses

Creditworthiness Review

- Recommended for new Individual Billed Account (IBA) applicants (OMB Circular A-123, appendix B)
 - Applicant agrees or refuses U.S. Bank to conduct a credit score check.
 - Applicant Refusal = Restricted Card
 - \$2,500 limit and reduced cash availability
 - Applicant Agrees to Credit Check
 - \$5,000 limit – cash 33% of monthly limit
 - Standard Card requires FICO > 660

Creditworthiness Review (Continued)

- 95% of IBA losses from January – December, 2011 were from accounts with a credit score < 660
- 73% of losses on individual travel charge cards are on accounts opened within the past two years
 - Important to assign appropriate limits and proper card access at account initiation

Suspension/Cancellation/Dunning

Number of Days Past Due:	Result:
30 days (past due one payment)	Statement message
45 days	Pre-suspension code applied and letter sent to cardholder
55 days	Second pre-suspension letter sent
60 days (past due two payments)	Suspension code applied and statement message

Suspension/Cancellation/Dunning (Continued)

Number of Days Past Due:	Result:
90 days (past due three payments)	Pre-cancellation/salary offset letter sent and statement message
120 days (past due four payments)	Pre-cancel code applied and letter sent
126 days	Cancel code applied and letter sent. Late fee calculation of 2.5% of amount 120+ past due.
150 days (past due five payments)	Pre-charge off letter sent

Collection Calls

- Cardholders 16-59 days past due are downloaded into the Collection Management System and collected via the auto dialer
 - Prioritized high to low balance with broken promise accounts addressed first
- Cardholders 60-89 days past due are assigned to individual collectors. Collector provides variety of options to help customer pay the balance

Collection Calls (Continued)

- Cardholders 90 - 119 days have outbound calls made with increased frequency and intensity. Cardholders informed of the negative impact to their credit
- Cardholders 120 – 149 days past due have increased frequency and tone intensity as credit loss risk intensifies
- Customers receive final warning prior to charge-off
- Charged off accounts are referred to the U.S. Bank recovery team, and credit reporting agencies are notified

Salary Offset - Description

- Salary Offset is the process by which government agencies garnish wages of employees with delinquent outstanding balances on their IBA travel cards
- Many agencies do not begin garnishment of wages until the account is 121 days past due
 - Once a cardholder enters into Salary Offset, U.S. Bank discontinues other collection and recovery efforts and the cardholder's wages will be garnished by the Agency until the past due balance has been paid in full

Salary Offset - Process

- U.S. Bank sends cardholder a Salary Offset Letter when the account balance is 90 days past due
 - This letter notifies the cardholder that their wages may be garnished if payment in full is not made
- U.S. Bank sends cardholder a Salary Offset Letter when the account balance is 90 days past due
 - Agency will notify all 90 day Past Due cardholders of their rights to an appeal to the Salary Offset process
 - Agency will review appeal requests, validate that a client is eligible for offset

Salary Offset – Process (Continued)

- A report of all 120 days past due cardholders is sent to the Access Online secured mailbox
 - Agency reviews the report and removes any cardholders that have successfully appealed their late balances or those others that should not be included in the Salary Offset process

Salary Offset – Process (Continued)

- Day 125, the Agency submits finalized Salary Offset report to U.S. Bank
 - Within 5-7 business days of receipt, if applicable, U.S. Bank assesses the Agency Salary Offset fee
 - Agency works with their payment/payroll processor to begin garnishment
- 125-150 days past due – the payment processor will begin sending cardholder offset payments to U.S. Bank



Disputes

Disputes

- Definition-
 - Cardholder does not recognize a transaction or has been unable to resolve an erroneous billing to their credit card
- Cardholder requirements-
 - Must attempt to resolve with the merchant
 - Provide detailed explanation to U.S. Bank
 - Notify U.S. Bank within 90 days of transaction date
 - Respond promptly to additional detail requests

Valid Disputes are...

- Duplicate charge
- Merchandise/services not received
- Returned merchandise
- Cancelled transactions/services
- Incorrect amount
- Paid by other means
- Defective merchandise
- Quality of service/merchandise
- Unrecognized/unauthorized
 - Unauthorized requires the account to be closed

Invalid Disputes are...

- Sales tax
- Shipping & handling
- Exchange rates
- Convenience checks
- Credits/re-bills
- Government service rebates
- Different fiscal year
- Wrong customer's account
- Unofficial/unauthorized cardholder purchases, cardholder abuse

Dispute Timeframes

- Guidelines

- To preserve dispute rights, a dispute must be received within 90 days from the date on which the transaction posted
 - Draft requests, that have not been officially disputed, do not preserve your dispute rights
- Unauthorized transactions by the cardholder should be called in as a fraud case, since the account will need to be closed before we can assist

Dispute Process

- Cardholder disputes transaction
 - Dispute reason
 - Identify reason for the transaction dispute
 - Submit relevant information/documentation
- Transaction is suspended
- Dispute case is researched
 - Visa/MasterCard regulations
 - Additional information obtained/requested
 - Obtain transaction receipt
 - Contact customer

Dispute Process (Continued)

- May charge back to merchant
 - Cardholder receives provisional credit
- Merchant rebuttal
 - Up to 45 days from chargeback date
 - Additional information
- Updated cardholder response
- Pre-arbitration/arbitration

Transaction/Disputes

- Resolved in favor of cardholder – credit issued
- Resolved in favor of merchant – no credit
- All disputes, whether they were initiated in Access Online or not, will appear on the Transaction List Report

Name	Account Number	Managing Account	Trans Date	Posting Date	Cycle Close D:	Trans Amount	Disputed	Dispute Status	Dispute Status Date	Merchant Name
JOE COOL	*****000111111	*****4555592511	2008/05/28	2008/05/29	2008/06/19	\$139.00	Y	Unresolved		ZAP*ZAPPOS.COM
JOHN SMITH	*****100011112	*****4555592578	2008/05/12	2008/05/13	2008/05/19	\$88.15	Y	Resolved in Favor of Cardholder	2008/05/22	GSA-FSS-ADV
JOHN SMITH	*****100011112	*****4555592578	2008/05/12	2008/05/13	2008/05/19	\$88.15	Y	Resolved in Favor of Cardholder	2008/05/22	GSA-FSS-ADV
JANE DOE	*****000111113	*****4555599573	2008/05/27	2008/05/27	2008/06/19	\$9.10	Y	Resolved in Favor of Merchant	2008/07/01	CENTER COMPANY
BOB JOHNSON	*****000111114	*****4556159211	2008/05/15	2008/05/19	2008/05/19	\$359.40	Y	Resolved in Favor of Merchant	2008/05/28	STARTLOGIC, INC
ANN OLSON	*****000111115	*****4556565862	2008/06/02	2008/06/03	2008/06/19	\$112.29	Y	Unresolved		STANLEY SUPPLY & SVCS

How to Initiate a Dispute

- Access Online

<https://access.usbank.com>

- Customer Service

888-994-6722

- Mail

U.S. Bank Government Services

PO Box 6347

Fargo, ND 58125-6347

- Fax

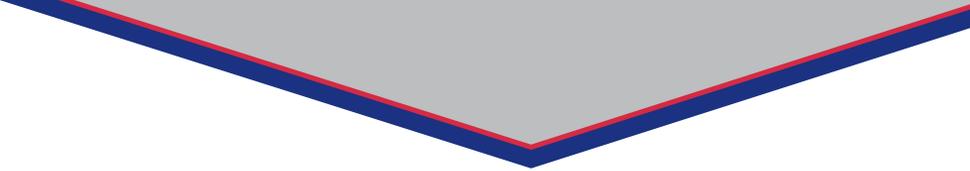
866-457-7506

Documents

- Please contact your Relationship Manager for documents regarding:
 - Account Security Tips
 - Fraud and Disputes Process



Questions?



Thank You

Presentations are available now on
www.usbank.com/sp2presentations

Complete a survey on this session at:
www.gsasmartpayconference.org/survey