SCTEM

Preventing Fraud and Misuse in Your Card Program

Presented By:

Gonca Latif-Schmitt, Managing Director
Citi

Agenda

- Card Misuse vs. Card Fraud - Definition
- Card Misuse
- Card Program Risks
- Fraud Types
- Fraud Partnership and Prevention
- Data Stream Compromises
- Fraud Technology
- ATM Skimming
- Fraud Prevention Practical Tips
- Questions

Overview of Fraud Session

- The goal of this session is to provide you with an overview of various types of fraud and card misuse/abuse.
- Provide best practices to protect your organization's card program from fraud loss, including a review of product design, and understanding the risk factors.
- Identify and define strategies to prevent external fraud and internal card misuse and abuse
- Increase your awareness of the services and support that your provider has built to assist you to safeguard your card programs against fraudulent transactions.

Background on Fraud in the Credit Card Industry

Credit Card Fraud occurs when one individual (fraudster) illegally obtains the account number of another individual – with the intent to fraudulently utilize the card for purchases.

- Credit Card Fraud is an industry-wide issue. Issuers, Acquirers, Merchants and Consumers all work toward fraud prevention, but over the years, the fraudsters have become more and more sophisticated.
- There are several different ways that Fraudsters illegally obtain credit card numbers:
  - Application Fraud – when an individual falsifies a credit card application (Rare in Commercial Card)
  - NRI – Never received reissued or new card (These cards are intercepted before being delivered to the legitimate cardholder)
  - Lost – Cardholder misplaces / loses card
  - Stolen – Cardholder is victim of theft
  - Skimming – Fraudsters will use a device to obtain account numbers. Often times this device is over layered on a regular swipe pad.
  - Phishing – Fraudsters send emails or make phone calls to attempt to get cardholders to provide personal data

Fraud

- According to the FBI, the number of victims will increase by 500,000-700,000 each year
- Every 79 seconds an identity is stolen
- 28% of identity theft was due to a lost or stolen credit card
- New and more brazen attempts are drugging travelers, in restaurants, bars, on trains, etc.
  - The individual's card is pulled and used immediately before being replaced on the traveler
  - Cardholder may not be aware of fraudulent charges until the statement is generated

Misuse/Abuse and Fraud Defined

- Misuse/abuse
  - Cardholder uses his/her own card for transactions not permitted by policy
  - Payment of all transactions falling into this category are the responsibility of the University

- Fraud
  - A person or entity other than the cardholder makes a transaction using the cardholder's account without the knowledge/consent of the cardholder
  - University is NOT financially responsible for these types of transactions and must follow their providers instructions on disputing process

Typically, commercial card vendors have an electronic dispute process that consists of obtaining signed affidavits and documentation within a certain time frame

Types of Misuse - Defined

- Personal Spending
- Late expenses
- Incorrect Merchant codes
- Violations of policies
- Dollar limit violations
- Splitting transactions

Misuse — Staff Personal Spending

- In the current economic environment, organizations should be alert to increased commercial card abuse and misuse, as personal expenses increase and personal income may decline.
- Organization's can put a few simple rules in place to curb potential escalating card misuse:
  - Deliver very clear, simple and frequent messages to cardholders – “No personal spending is allowed”
  - Issue a clear policy on why NO personal spending is allowed on your cards
  - Place a formal document on your intranet site to increase policy awareness
  - Back up the policy with adequate disciplinary action as a consequence of misuse
- Use the data resources of your provider to support you and to review MCC code spend
- Be suspicious of late expenses, which can later become a “dispute”

Preventing Misuse and Abuse in Your Card Program

Establishing and Maintaining Controls

- Establish POLICIES to prevent misuse by explicitly outlining: Timeframes for canceling inactive cards and cards for exiting / retiring employees
- Who should receive a card?
- Entitlement Rights: Who should have authority to make changes to accounts
- Controls on cards – credit limit, single purchase limit, velocity limits, merchant category code groups, restricted card limits, etc.
- Expense Reporting System – tie in travel policy
- Cash Advance limits / controls

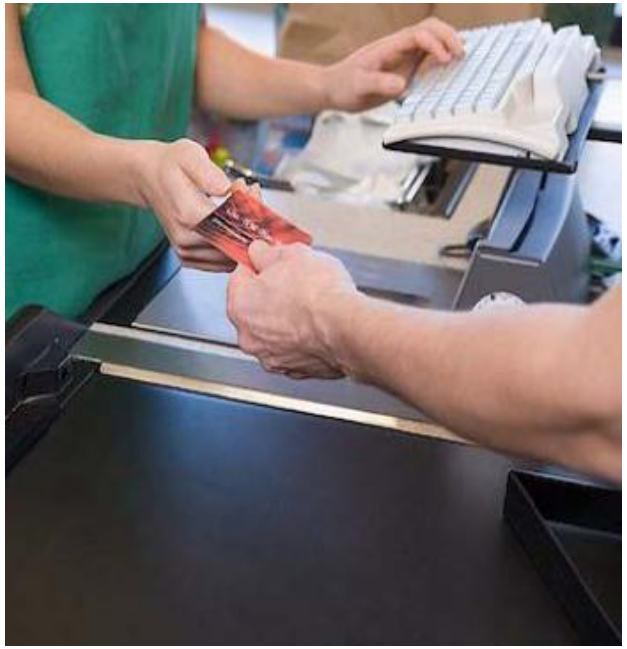
Preventing Misuse and Abuse in Your Card Program

Establishing and Maintaining Controls

- Establish PROCEDURES to prevent misuse by explicitly outlining:
  - How to cancel cards for exiting employees
  - How to determine if unauthorized users have access to cards
  - How to obtain, change and close an account
  - Policy training for users
  - Reconciliation process
  - Audit process and frequency
  - Authorization controls

Policy Reinforcement

- Document and update all policies for your program
- Manage delinquency
- Implement proper training for cardholders (new cardholder and refresher training)
- Maintain training certificates in a database or personnel records
- Tie policy violations to human resource actions (i.e. suspensions and or terminations of employment)



Misuse - Card Program Risks

- At the beginning of any new project the question of payment type arises
- Companies believe they will suffer less fraud (internal and external), if the individual pays and claims expenses
- Facts
  - Individual Pay cards statistically have a higher level of personal spend and create a greater third party fraud risk, than Company Pay
  - High risk means more incidence of card replacement and bad feedback
  - Higher incidences of late fees
  - Higher increase in write-offs
  - Impact on the card program's rebate
- Common Cardholder Misconceptions
  - There is an emotional link with the plastic and payment of the monthly bill for a cardholder and it is common across the globe
    - "It's alright to use my Corporate Card for personal expenses. If I pay the bill and claim back, it's my card and not the company's."

Fraud Types

- Compromised
  - Account numbers, expiration dates and CVC2 details are used online to make internet purchases
- Counterfeit
  - The card has been ‘skimmed’ with it’s magnetic strip and a copy of the card is used to make purchases
- Lost/Stolen
  - Card is lost or stolen – Early notification of lost/stolen card is key
- Not Received (Lost in Mail)
  - Not as frequent as other fraud types but does occur and should not be underestimated
- Account Takeover
  - Attempt by a third party to utilize a cardholder’s account

Partnering with Your Vendor to Manage Fraud and Misuse

In summary what can they do to help?

- **Example of what to look for from your provider**
  - **Account Monitoring**
    - Dedicated and experienced Fraud Early Warning team
    - Customer Service vigilance and knowledge of your program and its needs
    - 24/7/365 Cardholder and Program Administrator support
- **Communication**
  - Proactive client communication if and when suspicious activity occurs

Data Stream Compromises

- A global issue for all credit card companies and their clients
- Usually computer based
- Higher volume of affected accounts
- Generally perpetrated through merchant acquire process
- Data “hacks” merchants (i.e., the T.J. Maxx and Heartland Payment Systems fraud cases) undermining the brand value and impacting cardholder confidence

Data Stream Compromises (continued)

- In Europe (as part of a pilot) we now list all cards on an “alert” warning and compare against our fraud cases, so we can assess exposed risk against future risk
- If the number of cards where fraud has occurred exceeds a threshold that your provider feels is unacceptable, then the provider will advise their clients
- Providers will typically call cardholders if the risk is accelerated i.e. if fraud is actually happening now, in real time
- This process benefits cardholders who are traveling by not disrupting their service and preventing them from using their cards when they need it the most.
- Program Administrators (PA’s) are informed
- Number of reissued cards are reduced based on our experience and ability

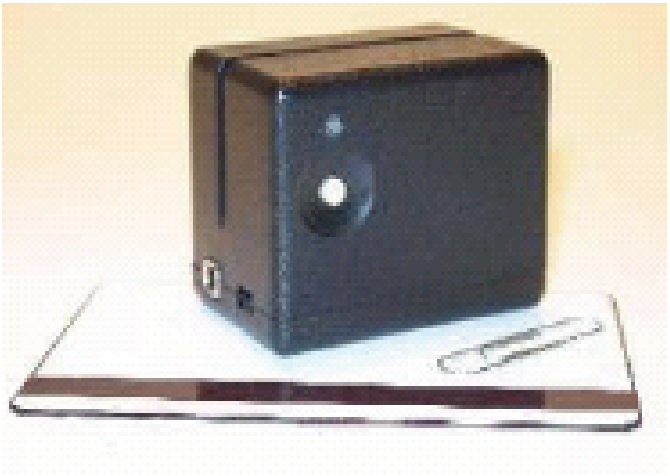
Fraud Technology

- Most providers operate several fraud prevention systems to detect suspicious transactions
- They will assess the following on an ongoing basis:
  - Spend patterns
  - MCC trends
  - Exchanges suspicious merchant details across the globe
- Your provider should be continually reviews card activity to improve security and provide a positive cardholder experience
- Most providers are active in lobbying the associations to develop ongoing security safeguards

ATM Skimming—What is a Suspicious Device?

- What is “skimming”?
  - Any terminal that reads and copies your magnetic stripe
  - A false cover over an ATM card insert slot, or a waiter with a small machine in his hand
- Why steal your card when an extra swipe with a small hand-held device will create a copy and you will not report any loss?
- A skimmer pulls the data from your card, giving the thief all the information needed to make a counterfeit card. A skimmer can hold card data from hundreds of cards. This information can be downloaded into a computer and e-mailed anywhere in the world
- Remember this applies to business cards not just to personal cards
- Do you ever check your local ATM or rail ticket machine where you live?

ATM Skimming—What does a Skimmer Look Like ?



Now Technology Allows the Camera to be Even Smaller …

Could You Spot the Camera?

Now What was Your PIN Number Again?

Drive-in ATM's

The gentleman in the photograph is a policeman collecting evidence, honestly

Fraud Partnership and Prevention

- Partner with your provider to leverage their fraud prevention expertise
- Your provider can assist you in product design training and work with you to ensure your card program transactions do not appear on the “fraud radar”.
- Do you have a Specialist Department, Product Buyers or senior executives who travel frequently?
  - You can work with your provider to organize additional training, conference calls and discuss new methods for supporting your cardholders whether they travel around the block or around the world.

Fraud Partnership and Prevention

- Ability for your provider to communicate to your cardholders is key
- Your provider needs to be able to reach cardholders, their assistants, or PA's, as soon as possible to protect the cardholder
- Essential tools are:
  - E-mail and Cell phone
- With these tools your provider can:
  - Get a cardholder home
  - Protect a client from continued fraudulent transactions
  - Keep your business going
- Fraud Specialists:
  - Help you to mitigate risk
  - Reduce declines
  - Support your cardholders during a fraud episode
  - Can work with you to prevent fraud from occurring again

Fraud Prevention Practical Tips

Fraud Prevention Practical Tips

- Rigorously check your monthly card billing statements
- Contact your provider immediately if there are unrecognized transactions on your statement
- Do not throw away card receipts (check them against your statement)
- Never leave your cards in an unlocked desk or drawer
- Be careful when providing card information (such as PIN number or passwords) to another person
- Avoid letting merchants take your card out of sight
- Use your card only for authorized use as defined by your organization
- Keep your account contact information up to date
- Do not keep your PIN in your wallet or purse
- Do not use common personal information, such as date of birth, for a password/PIN

QUESTIONS

DO YOU HAVE ANY QUESTIONS?

IRS Circular 230 Disclosure: Citigroup Inc. and its affiliates do not provide tax or legal advice. Any discussion of tax matters in these materials (i) is not intended or written to be used, and cannot be used or relied upon, by you for the purpose of avoiding any tax penalties and (ii) may have been written in connection with the "promotion or marketing" of any transaction contemplated hereby ("Transaction"). Accordingly, you should seek advice based on your particular circumstances from an independent tax advisor.

Any terms set forth herein are intended for discussion purposes only and are subject to the final terms as set forth in separate definitive written agreements. This presentation is not a commitment to lend, syndicate a financing, underwrite or purchase securities, or commit capital nor does it obligate us to enter into such a commitment, nor are we acting as a fiduciary to you. By accepting this presentation, subject to applicable law or regulation, you agree to keep confidential the information contained herein and the existence of and proposed terms for any Transaction.

Prior to entering into any Transaction, you should determine, without reliance upon us or our affiliates, the economic risks and merits (and independently determine that you are able to assume these risks) as well as the legal, tax and accounting characterizations and consequences of any such Transaction. In this regard, by accepting this presentation, you acknowledge that (a) we are not in the business of providing (and you are not relying on us for) legal, tax or accounting advice, (b) there may be legal, tax or accounting risks associated with any Transaction, (c) you should receive (and rely on) separate and qualified legal, tax and accounting advice and (d) you should apprise senior management in your organization as to such legal, tax and accounting advice (and any risks associated with any Transaction) and our disclaimer as to these matters. By acceptance of these materials, you and we hereby agree that from the commencement of discussions with respect to any Transaction, and notwithstanding any other provision in this presentation, we hereby confirm that no participant in any Transaction shall be limited from disclosing the U.S. tax treatment or U.S. tax structure of such Transaction.

We are required to obtain, verify and record certain information that identifies each entity that enters into a formal business relationship with us. We will ask for your complete name, street address, and taxpayer ID number. We may also request corporate formation documents, or other forms of identification, to verify information provided.

Any prices or levels contained herein are preliminary and indicative only and do not represent bids or offers. These indications are provided solely for your information and consideration, are subject to change at any time without notice and are not intended as a solicitation with respect to the purchase or sale of any instrument. The information contained in this presentation may include results of analyses from a quantitative model which represent potential future events that may or may not be realized, and is not a complete analysis of every material fact representing any product. Any estimates included herein constitute our judgment as of the date hereof and are subject to change without any notice. We and/or our affiliates may make a market in these instruments for our customers and for our own account. Accordingly, we may have a position in any such instrument at any time.

Although this material may contain publicly available information about Citi corporate bond research, fixed income strategy or economic and market analysis, Citi policy (i) prohibits employees from offering, directly or indirectly, a favorable or negative research opinion or offering to change an opinion as consideration or inducement for the receipt of business or for compensation; and (ii) prohibits analysts from being compensated for specific recommendations or views contained in research reports. So as to reduce the potential for conflicts of interest, as well as to reduce any appearance of conflicts of interest, Citi has enacted policies and procedures designed to limit communications between its investment banking and research personnel to specifically prescribed circumstances.

.

In January 2007, Citi released a Climate Change Position Statement, the first US financial institution to do so. As a sustainability leader in the financial sector, Citi has taken concrete steps to address this important issue of climate change by: (a) targeting $50 billion over 10 years to address global climate change: includes significant increases in investment and financing of alternative energy, clean technology, and other carbon-emission reduction activities; (b) committing to reduce GHG emissions of all Citi owned and leased properties around the world by 10% by 2011; (c) purchasing more than 52,000 MWh of green (carbon neutral) power for our operations in 2006; (d) creating Sustainable Development Investments (SDI) that makes private equity investments in renewable energy and clean technologies; (e) providing lending and investing services to clients for renewable energy development and projects; (f) producing equity research related to climate issues that helps to inform investors on risks and opportunities associated with the issue; and (g) engaging with a broad range of stakeholders on the issue of climate change to help advance understanding and solutions.

Citi works with its clients in greenhouse gas intensive industries to evaluate emerging risks from climate change and, where appropriate, to mitigate those risks.