



Managing and Mitigating Card Fraud

Matthew Cissne, Bank of America Merrill Lynch

March 13, 2013



Agenda

- Welcome
- Definitions
- Data Breaches
- Phishing
- Managing Fraud
- Best Practices
- Questions and Answers

Fraud, Abuse, & Misuse: Definitions

Fraud – The theft of card information by fraudsters

- Account takeover (information change)
- Counterfeit cards
- Lost/Stolen cards
- Card Not Present
- Skimming
- Database Hacking
- Franchise Software Hacking
- Phishing

Abuse – Intentionally or unintentionally violating policies and procedures for personal gain

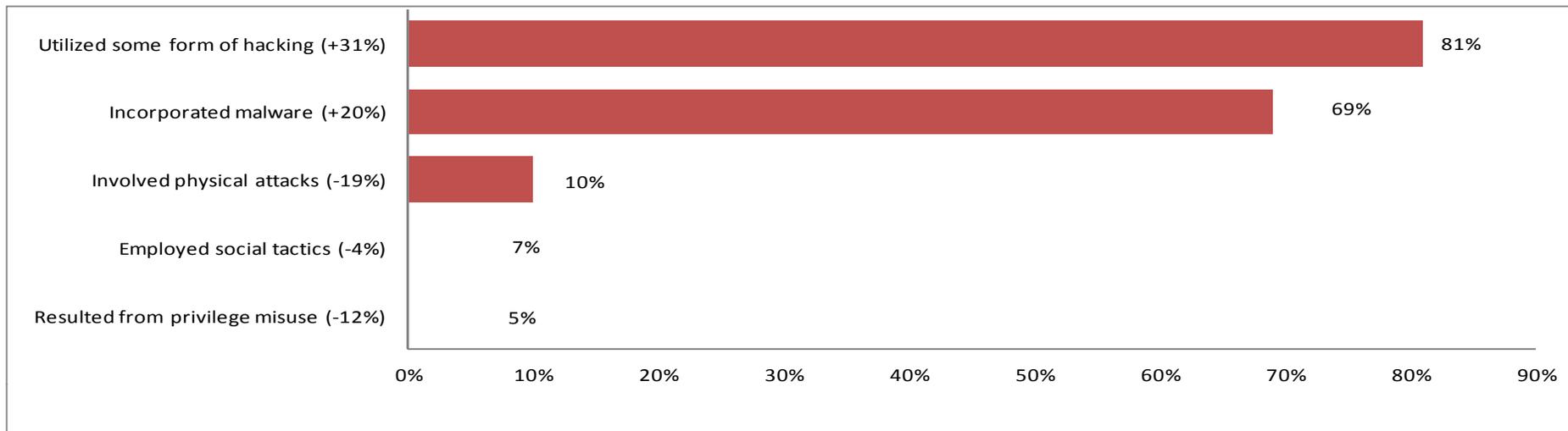
Misuse – Intentionally or unintentionally violating policies and procedures for work related gain



Data Breaches

Industry Data Breaches

How Do Breaches Occur?



Data: Verizon 2012 Data Breach Investigations Report (percentages in parentheses represent change from the 2011 report)

Fraud Definitions:

- **Hacking** – Act of breaking into computer systems to access or harm data without authorization
- **Malware** – Slang for malicious software which may include emails including links that open to web pages or PDF, pop up windows, free software, which are all ploys used to exploit data; may include key logging virus or spyware that records all keyboard activity
- **Physical Attacks** – Encompasses internal employee actions that require physical proximity to servers or PCs to obtain data or tapping with point-of-sale terminals
- **Social Attacks** – Tactics that employ deception, manipulation, intimidation to exploit the human element can be with monetary rewards but most common data obtained is sold underground as hot commodities
- **Privilege Misuse** – Internal data access that may be intentional or unintentional including embezzlement, skimming, and system abuse

External Data Compromise Fraud Servicing Actions

- **Ongoing Servicing Mitigation**

- Immediately monitor all transaction activity within fraud to prevent high risk activity
- Notify cardholders and clients that require card to be replaced
- As appropriate, conduct exception processing to accommodate cardholder special requests, including overnight plastics to expedite receipt of cards

- **Cardholder Notification**

- Recent change in certain state laws mandate that entity must notify cardholders of data breach
- May result in client/cardholders being informed before bank targets accounts for replacement
- Notification may come from a 3rd party vendor or via media notification (i.e. press release or internet)

- **External Data Compromise Fraudsters are patient in leveraging data obtained**

- **Action for Cardholders**

- If concerned, please contact your Bank of America representative or Fraud department at (866) 500-8262 or the telephone number on the back of your card



Phishing

Phishing

Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

-----Original Message-----

From: Bank of America Alert
[mailto:onlinebanking@alert.fraud.edu]
Sent: Sunday, May 09, 2010 4:55 PM
To: Cissne, Matt
Subject: Bank of America Alert: Irregular Credit Card Activity

Dear Customer:

**We detected irregular activity on your Bank of America credit card on 09/May/2010.
To safeguard your account, we've classified it as dormant.**

What does this mean for you?

You will not be able to use your credit card, until it has been reactivated. The process for reactivation is simple:

- 1. Download the activation form.**
- 2. Enter basic security information**

Don't forget - your credit card can be used anywhere VISA® or MasterCard® is accepted so once you've reactivated your account, you're free to spending money.

If you do not reactivate your account, your account will remain dormant.

Yours sincerely,

Bank of America 
Merrill Lynch

Phishing Emails/Telephone Calls

Ways to identify Phishing from Bank of America Merrill Lynch contacts

- Bank of America Merrill Lynch will not ask cardholder to provide account number and/or personal information via an email
- Most fraudulent communications convey a sense of urgency by threatening discontinuing service or declining authorizations
- Many fraudulent emails contain misspellings, incorrect grammar, and poor punctuation
- Links within the email may appear valid, but deliver you to a fraudulent site
- Phishing emails often use generic salutations like "Dear Customer," or "Dear account holder" instead of your name
- All legitimate Bank of America Merrill Lynch emails will include telephone number to contact office

Actions for Cardholders

- Do not provide sensitive data via e-mail or unsolicited web page
- Forward any emails if received to abuse@bankofamerica.com
- If concerned, please contact your account manager, the Fraud department at (866) 500-8262 or the telephone number on the back of your card

Example of legitimate fraud alert e-mail

Email Verbiage

From: bankofamericaalert@bankofamerica.com [mailto:bankofamericaalert@bankofamerica.com]

Sent: Tuesday, September 13, 2011 3:45 PM

To: Jones, Paul

Subject: Bank of America: Important Information for Paul Jones

This email is intended for Paul Jones only. If you are not this person, please delete this email.

Regarding account number ending in: 1234

Dear Paul Jones:

We are committed to the security of our customers' accounts. In an effort to protect the above referenced account, we would like to discuss recent activity.

Please call us toll-free at 1.877.451.4602 or if you are traveling internationally call us collect at 1.509.353.6656, as soon as possible. Our knowledgeable associates are available 24 hours a day, seven days a week to assist you.

Thank you for your prompt attention to this matter.

Please do not reply to this email as this mailbox is not monitored

Mobile

Emerging Risk

- Smartphone users are the 1st to follow phishing emails
- 3 times more likely to provide log in information from device than accessing internet from PC
- Mobile Malware on the rise specifically for Google's Android
- 400% increase in Fraud from 2010; 4% of total fraud in 2011
- Encouraging tidbit is #1 attacked industry continues to be financial industry and most users do not retain financial data on smartphones but risk emerging
- Lost and stolen devices a growing concern; industry mitigating by adding tracking devices to phones to locate
- Industry working together to find tools to combat risk

Source: Dark Reading Fraud on Mobile Devices Revealed 2011

Managing Fraud



Fraud Servicing Scenarios

Authorizations that Fraud Needs to Validate

- Outbound Call to Primary Contact listed on account to verify activity
- If no answer, Outbound Call to Secondary contact listed on the account
- If no answer at either telephone numbers or outside of calling hours, email sent to primary contact

Posted Fraud Charges that Require Credit

- Following fraud confirmation, the account will be closed and each transaction transferred to new account
- All transactions will appear on the new account number billing statement or your reporting tool
- Fraud Claims may send a fraud statement to the PA or cardholder via email, fax or regular mail
- PA asked to complete Fraud Affidavit to comply with VISA and MasterCard regulations
- Credits for individual fraud transactions will appear on new account for balance reconciliation

Actions for Clients

- Fraud department 866-500-8262 or collect 509-353-6656 is available 24/7 to assist with questions or verification

Misuse/Abuse Insurance

Requirements for Service

- Free Misuse/Abuse Insurance service for clients with use of commercial card program
- Associate involved must be terminated to qualify for insurance coverage
- Association covers 75 days prior to termination and 14 days after
- \$100,000 per cardholder
- No exclusion on transaction types

Posted Abuse Charges that Require Credit

- Notify Bank of America Merrill Lynch of account closure or complete cancelation of account ASAP to protect interests
- Contact Fraud team to determine next steps with possible recovery efforts
- Association requires form and supporting documents to be provided to file Claim
 - Verification of associate dismissal
 - Itemization of the charges that are involved in case
 - Standard form to be completed
- Bank of America Merrill Lynch files paperwork with the association on your behalf
- Bank of America sends demand letter to cardholder involved as component to Visa requirements
- Subsequent credit will be applied to credit card account
- Expect 30–60 days for resolution

Fraud Success

Industry Recognition

- Ranked #1 for Fraud Prevention by Javelin Strategy and Research for last 6 years (Top 26 card issuers screened)¹
- Consistently achieve < 3 bps of fraud compared to Transaction Volume for last 5 years (Industry Average 6 bps)
- Leader in Industry Forums regarding Fraud Mitigation strategies

Internal 2011 Results

- Balance Client Experience and fraud mitigation in every decision
- Achieved 90+% Satisfaction Rating from our Clients in Fraud Survey in 2012
- 99.8% of all transactions decisioned by fraud were successfully completed by our customers
- Continue to invest in industry leading tools to mitigate fraud and reduce impact to our clients
 - Visa Advanced Authorization Score
 - MasterCard Expert Score
- Provide custom fraud solutions to assist clients as needed

Source: 1.) <https://www.javelinstrategy.com/>



Best Practices

Vendor Services and Mobile Technology

Vendor Services

- Perform site review and engage all resources to assist in decision making
- Review internal needs and allow vendor access only to required data and limit log-ins to limit potential breaches
- Ask and understand the vendor's loss recovery processes and service level agreements currently in place
- Do your homework – check references, awards, or company standards regarding product and data security processes and procedures to ensure a balanced risk/reward decision

Mobile Devices

- Choose devices carefully – select device that provides encryption and authentication capabilities
- Use Intrusion Prevention software
- Control and limit third party applications downloads
- Limit Bluetooth capabilities – switch to hidden or turn off broadcast when not in use
- Avoid using an automatic login features that save usernames and passwords for online banking

Card Industry Best Practices

Client Controls

- **Create guidelines for card issuance and handling**
 - Determine who should be eligible to apply for a card
 - Determine approval levels required
 - Segregate duties of ordering and receiving of cards
- **Create internal procedures**
 - Requirements for obtaining a card
 - Administrative / Management
 - Usage / Purchasing
 - Accounts Payable/Accounting
 - Reconciliation
 - Audit
- **Create policies or business rules**
 - Business versus Personal Use
 - Cash access
 - Card sharing
 - Ghost cards
 - Roles and responsibilities
 - Training
 - Audit exceptions

Internal Audit Process

- Audits should be scheduled, random, and unannounced
- Audit representative samples - within 60-90 days
- Review span of control
- Focus resources on areas of weakness or opportunity
- Combine filter development and automation of monthly review process
 - Streamlines review and audit process
 - Eliminates the need for 100% transaction review
 - Documents the review process
 - Supports timely review of transactions within the span of control
 - Improves the recovery potential
- Improve communication of audit findings to card program participants
- Develop a sampling audit strategy for current cycle transactions
- Audit the first statement cycle following cardholder training or change in process

Card Industry Best Practices (cont'd)

Sample Metrics

- **Audit high-risk transactions monthly**
 - Cardholders with the highest number of transactions
 - Cardholders with the highest dollar amount spent
 - Employees with multiple disputes
 - Purchases charged to clients
 - Increase frequency for those cardholders with exceptions Audit representative samples - within 60-90 days new account
- **Vendors**
 - Number of vendors utilized
 - Transactions per vendor
 - Transactions between a cardholder and same vendor
- **Reconciliation**
 - # and \$ of Transactions between a cardholder and same vendor
 - Review items not submitted or duplicate expense reports for same transaction
 - Accountable property transactions logged
 - Transactions from approved suppliers
 - Transactions reconciled using default funding
 - Split purchase occurrences to avoid dollar thresholds

Card Industry Best Practices (cont'd)

Program Administrator

- Ensure cardholder statement reconciliation is performed in a timely manner
- Monitor declined authorizations for signs of merchant and/or employee abuse
- Manage credit limits based on individual cardholder spending needs
- Consider MCC (Merchant Category Codes) restrictions and \$ thresholds to prevent internal and fraud abuse
- Complete internal audits of transaction monitoring at MCC and cardholder levels
- Provide Bank of America Merrill Lynch after hours contacts or cell phone telephone numbers and emails for prompt contact to detect and prevent fraud
- Partner with fraud team future or current authorization needs to improve control with least amount of cardholder impact

Cardholder

- Report non-received cards to Bank of America immediately
- Examine cards received for evidence of tampering during transit
- Do not provide your individual account number to a merchant to keep on file unless approved by company
- Contact Fraud team prior to international trips and provide alternate contact phone number as needed

Summary

Everyone Has a Role/Responsibility in Fraud Prevention

- Industry
- Organizations
- Financial Institutions
- Individuals
- Law Enforcement
- Media
- Other Interested Parties

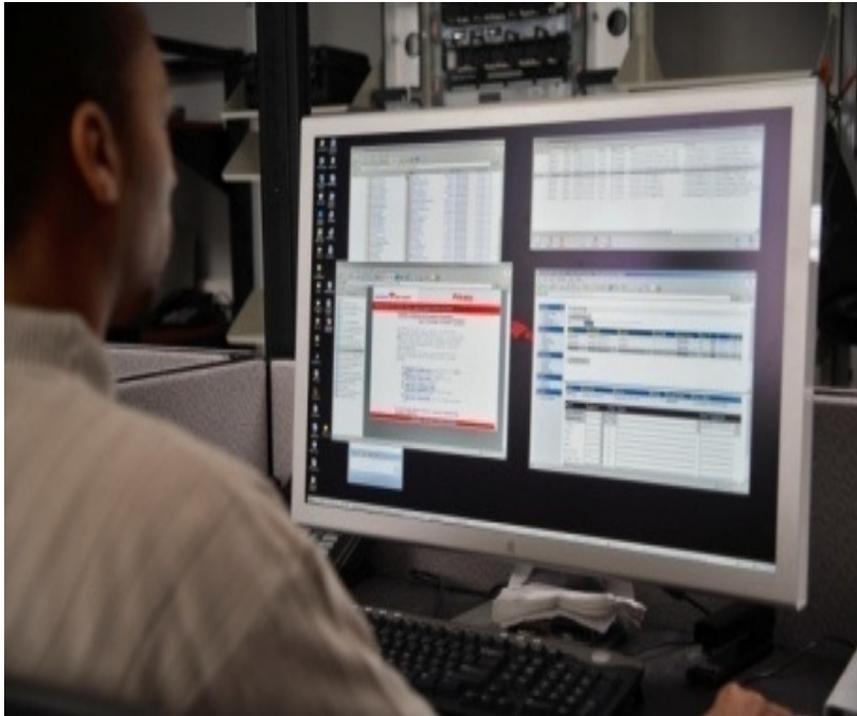
Be diligent in all transactions and vendor interactions

Contact your Bank of America representative to assist with concerns/questions



APPENDIX

Industry Best Practices for desktop security



- Be suspicious of emails requesting account information, account verification or banking access credentials
- Create strong passwords with 8 characters minimum
- Choose passwords that have a combination of alpha and numeric characters, change passwords frequently
- Log off/lock up computers when not in session
- Do not accept or complete automatic internet pop-ups
- Verify that website is utilizing secure session (https appears in the address window)
- Avoid using an automatic login features that save usernames and passwords for online banking
- Install and maintain anti-virus, anti-malware, spyware applications, and operating system patches

Industry Best Practices for Data Access



- Encrypt sensitive information, laptops, and removable storage devices
- Control how users access information
- Be careful that the devices of departing workers are securely wiped
- Install a dedicated, actively managed Firewall
- Limit network administrative rights for users
- Make certain computers are running all current operating system patches and updates to prevent unauthorized access
- Install and maintain real time anti-virus, anti-malware and spyware software applications

Identity Theft –Definition and Contacts

Identity theft occurs when someone uses your personal information including name and social security number without your permission to commit fraud or other crimes.

- Federal Trade Commission estimates 9 million identities are stolen each year
- Can impact ability to obtain housing, employment and bank accounts

Ways to identify ID Theft Identification

- Obtain annual credit bureau report to check for any unknown activity:
<https://www.annualcreditreport.com/cra/index.jsp>
- Negative changes in credit lines, interest rates or other unexpected changes to established accounts

Credit Bureau Contacts if you suspect ID Theft:

TransUnion: 1-800-680-7289; www.transunion.com Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Equifax: 1-800-525-6285; www.equifax.com P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com P.O. Box 9554, Allen, TX 75013

Identity Theft: Best Practices

- Avoid providing your Social Security Number unless you have initiated the request and confirmed the business and person's identity
- Do not list Social Security Number on checks or carry ID card in your wallet
- Monitor bank statements, credit card statements, and check your credit report
- Shred personal documents
- Never save credentials or personal information on unknown or community computers
- Guard your laptop, cell phone and other technology against theft
- Don't leave important mail sitting in physical mailbox
- When possible, request "Signature Required" when receiving sensitive mail via courier such as FedEx or UPS
- Be cautious when using the ATM by covering your PIN and taking your receipt, or don't request a receipt.



**Bank of America
Merrill Lynch**

