Reporting and auditing, can it really help you detect Card misuse and Fraud?

Kristen Bolden, Assistant Director, DOA
Maureen Sudbay, Card Account Manager BofA

Growing Commercial Card fraud trends

What's driving the security landscape?

DRIVERS

Innovation

>> Contactless cards
developing strategies to identify and mitigate fraud

Government

>> CNP regulations
new and pending requirements in all regions

Data Compromises

>> Account takeover
get personal information and create a new, fraudulent card account

EMV CARD TECHNOLOGY[1]

Helps reduce counterfeit cards.

>> 50+% decrease in counterfeit fraud[1]
>> 2MM chip enabled U.S. merchants[1]

TWO-WAY MOBILE ALERTS

Allows real-time notifications for selected events.

>> 30 minutes, instead of 2 days[2]

1 SOURCE: PYMNTS.com The Straight Scoop on EMV: One Year Later, September 2016
2 SOURCE: BofAML customer experience, "… quickly connected to a fraud specialist at Bank of America, and had a new card requested all in 30 minutes"

MONITORING TRENDS
Card tokenization

Setting the stage

Data Breaches

A data breach is an incident in which sensitive, protected or confidential data records, i.e. credit card numbers, customer data, SSN, etc., have potentially been viewed, stolen or used by an unauthorized individual.

Card Present

A face-to-face transaction at a "brick & mortar" merchant where the physical plastic card is presented for payment.

Typically the card is processed through a terminal with a magnetic stripe or PIN reader.

Card Not Present

An online or mail order/telephone order transaction where the card number is entered into a form or provided verbally. Sometimes a "CVV" number is requested to validate that the purchaser has access to the physical card. The PIN is never requested (and should never be provided) for a card not present transaction.

EMV (Chip & PIN) Impacts

Decrease in Card Present Fraud

- EMV added security to the payment card

Increase in "Old" Techniques

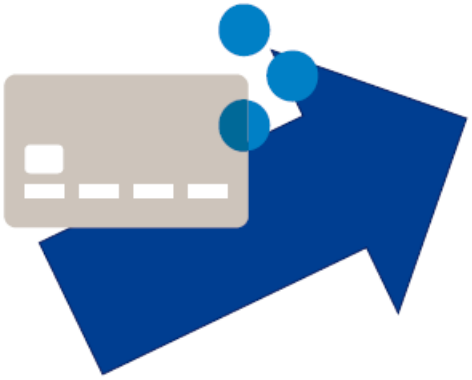
- Account takeovers
- Identity Theft
- Stolen Data

BofAML Experience

- 92% Overall US payment volume is on chip cards
- 55% of US storefronts are chip enabled
- 100% of BofAML clients are chip enabled
- Over 95% of BofAML Commercial Cardholders have a chip card in hand

Source: U.S. EMV Chip Monthly Update – July 2017 Snapshot

Card Not Present (CNP) Fraud



CNP Fraud is on the rise

- No physical card required
- Fraudsters can capture the information via data breaches

Evasive Actions

Merchants and Banks are implementing 3D Secure (Verified by Visa®, Mastercard® Securecode®)

Authorization process tied with an online cardholder authentication, expected to grow globally in the coming years

Practical fraud prevention tips and best practices

Client Controls

- Create guidelines for card issuance and handling
- Create internal procedures
- Create policies or business rules

Audit Best Practices

- Audit high risk transactions monthly
- Vendor Strategies
- Reconciliation

Program Administrators

- Make sure 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
- Work with fraud team future for current authorization needs to improve control with least amount of cardholder impact

Improved methods are required to combat a persistently changing fraud environment

TWO-WAY MOBILE ALERTS

- Allows real-time notifications for selected events
- Instantaneous notification of suspicious transactions via text, email, or automated call
- Faster resolution of suspected fraud activity

CUSTOM FRAUD SCORING MODEL

- Only uses BofAML client card authorizations data
- Allows fraud rules to be specific to Bank of America client base
- Learns and adapts to client spending patterns to minimize false positives

ENHANCED FRAUD DETECTION EMAIL

- BofAML branding eliminates phishing concerns
- Allows multiple email recipients
- Contains reference number that will be used for authentication and account identification
- Email sent during the detection review process versus batch processing

Leading the industry in fraud detection and resolution

ZERO liability for external fraud impacts

Fraud protection and monitoring
Dedicated team tracks trends and reviews activity

Account activity alerts through SMS, email or phone
Real-time notification of transactions

Employee misuse insurance
Consistent North America coverage as a best practice

Program control and spend monitoring
Exception reporting based on MCC codes

#1 FRAUD PREVENTION CARD SOLUTIONS

Javelin Strategy & Research, 2015

IDENTIFICATION	ANALYSIS	TREATMENT	OUTREACH
Identify points of compromise through internal and payment network processes	Analyze identified accounts Data type exposed Fraud type	Block and reissue Ongoing monitor of accounts	Coordinated reissue with administrators Proactive messaging to cardholder through email and phone

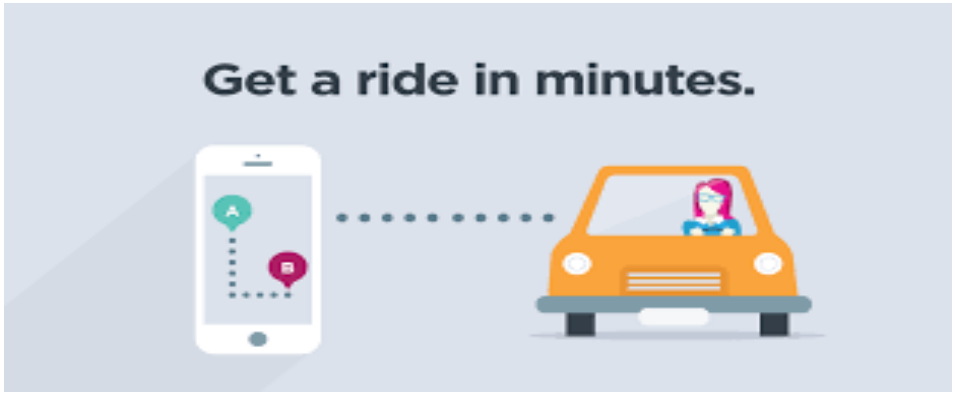
FORUM 2017

Real life examples of card misuse and tips to detect it

Third Party Payments…What's the Risk?

- Examples – PayPal, Square, & Stripe
- Allowable, but not the preferred method of payment
- Can pay through a third party system as long as card information is NOT stored

Questionable Vendors



lyft

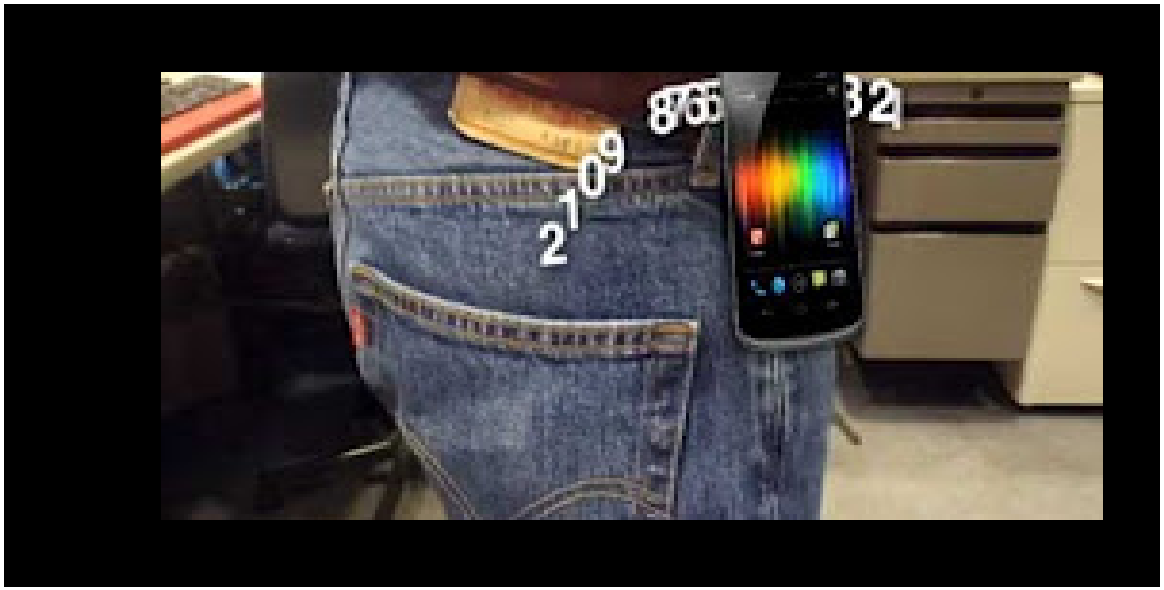
UBER

Fraud Examples

- Receipts- Statement manipulation
- PayPal- Payment to vendor with a personal name instead of business name
- Square- Payment to vendor with a personal name instead of business name
- Level 3 data- Look at payment details

Fraud Examples

Industry Fraud Trends



Suspicious Trends

- What are some suspicious trends you see???
- Multiple Transactions to the same vendor
- Multiple Credits received from the same vendor
- Increased number of Over-the-Counter purchases
- Frequent card replacements
- Diverting business funds
- Embezzlement of raw materials or

Types of Fraud

- Fraud trends
  - external
  - internal

If it is MISUSE….

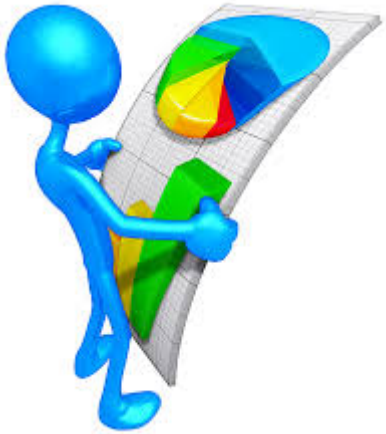
What's Next??????

- Immediately Contact Cardholder's Supervisor
- Alert DOA
- Suspend Card Immediately

Reports and Audits to detect Card misuse and Fraud on your program

Works Reports

- **Account Reports**
  - Card Declines
  - Card Status



- **Transaction Reports**
  - 13 Month Card Spend Analysis

- **Dashboard**
  - Audit

VISA IntelliLink Compliance

A web-based, modular application designed to provide analytics and investigative reporting; enable detection of potential misuse, abuse and potential fraudulent transactions; as well as ensure effective program compliance and management.

- **Rules**
- **Sampling**
- **Predictor**

What can you do to deter fraud?

Ways to deter Fraud

- Set appropriate monthly and single transaction limits
- Restrict by Merchant Classification Codes (MCC)
- Frequent reviews and approval of purchases by immediate supervisor
- Purchase reviews by a second person, the p-card coordinator
- Software monitoring to identify potential questionable transactions

The path forward

Fraud attempts will occur, but we are focused on minimizing impacts

Continued focus on balancing fraud risk while maintaining the highest level of client satisfaction

Let's work **together** to achieve a long-term, sustainable business model

Offer accurate contact information for your cardholders – including email address and phone number(s)	Enroll in account activity alerts for North America cardholders	Require fraud education and training, including phishing and masquerading

Implementing industry best practices has a positive impact on fraud deterrence

- Set company policies
- Review transactions and report suspicious transaction activity to bank immediately
- Segregate duties
- Differentiate user names and passwords across platforms
- Phishing & Masquerading – provide fraud education & training
- Client level fraud review – stats/trends/specific client experiences related to fraud

Notice to Recipient

"Bank of America Merrill Lynch" is the marketing name for the global banking and global markets businesses of Bank of America Corporation. Lending, derivatives, and other commercial banking activities are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Securities, capital markets, strategic advisory, and other investment banking activities are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, locally registered entities. Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.
This document is intended for information purposes only and does not constitute a binding commitment to enter into any type of transaction or business relationship as a consequence of any information contained herein.
These materials have been prepared by one or more subsidiaries of Bank of America Corporation solely for the client or potential client to whom such materials are directly addressed and delivered (the "Company") in connection with an actual or potential business relationship and may not be used or relied upon for any purpose other than as specifically contemplated by a written agreement with us. We assume no obligation to update or otherwise revise these materials, which speak as of the date of this presentation (or another date, if so noted) and are subject to change without notice. Under no circumstances may a copy of this presentation be shown, copied, transmitted or otherwise given to any person other than your authorized representatives. Products and services that may be referenced in the accompanying materials may be provided through one or more affiliates of Bank of America, N.A.
We are required to obtain, verify and record certain information that identifies our clients, which information includes the name and address of the client and other information that will allow us to identify the client in accordance with the USA Patriot Act (Title III of Pub. L. 107-56, as amended (signed into law October 26, 2001)) and such other laws, rules and regulations.
We do not provide legal, compliance, tax or accounting advice.
For more information, including terms and conditions that apply to the service(s), please contact your Bank of America Merrill Lynch representative.
Investment Banking Affiliates are not banks. The securities and financial instruments sold, offered or recommended by Investment Banking Affiliates, including without limitation money market mutual funds, are not bank deposits, are not guaranteed by, and are not otherwise obligations of, any bank, thrift or other subsidiary of Bank of America Corporation (unless explicitly stated otherwise), and are not insured by the Federal Deposit Insurance Corporation ("FDIC") or any other governmental agency (unless explicitly stated otherwise).
This document is intended for information purposes only and does not constitute investment advice or a recommendation or an offer or solicitation, and is not the basis for any contract to purchase or sell any security or other instrument, or for Investment Banking Affiliates or banking affiliates to enter into or arrange any type of transaction as a consequent of any information contained herein.
With respect to investments in money market mutual funds, you should carefully consider a fund's investment objectives, risks, charges, and expenses before investing. Although money market mutual funds seek to preserve the value of your investment at $1.00 per share, it is possible to lose money by investing in money market mutual funds. The value of investments and the income derived from them may go down as well as up and you may not get back your original investment. The level of yield may be subject to fluctuation and is not guaranteed. Changes in rates of exchange between currencies may cause the value of investments to decrease or increase.
We have adopted policies and guidelines designed to preserve the independence of our research analysts. These policies prohibit employees from offering research coverage, a favorable research rating or a specific price target or offering to change a research rating or price target as consideration for or an inducement to obtain business or other compensation.
Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor. No information contained herein alters any existing contractual obligations between Bank of America and its clients