5 Ways to Shape your Pcard Program to be “Best in Class”

Presented by:
Kristen Bolden, CPCP

DOA
Virginia Department of Accounts

Photo by Karl Steinbrenner

Financial Accountability. Reporting Excellence.

Agenda

- Process Improvements
- Securing your Role
- Separation of Duties
- Third Party Payments
- Audits/Card Fraud

Process Improvements

How to improve your process…

- Roles (From PA, Supervisor, & Fiscal perspectives)
- Online Reconciliation including receipts imaging
- Spot auditing
- Payment Center
- Accountability
- Examples

Securing your Role

- Cardholder- Payment –VS-Procurement
- Manager/supervisor- signing off on any transaction whether its OLR or traditional, you are verifying that you have reviewed the transaction, statement, reconciliation, and this is an approved purchase. You are also verifying that all coding and back-up documentation is correct.
- PA responsibilities- Following CAPP Manual
- Examples- Purchasing online instead of the eVA mall. Frequent over the counter purchases at non eVA vendors.

Separation of Duties

- Acquiring an SPCC
  - What is the process? Can a PA have a card?
- Review Process
  - How many levels of review are needed/required?
- Example

Third Party Payment Systems

- 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

PayPal™

Square

Audits

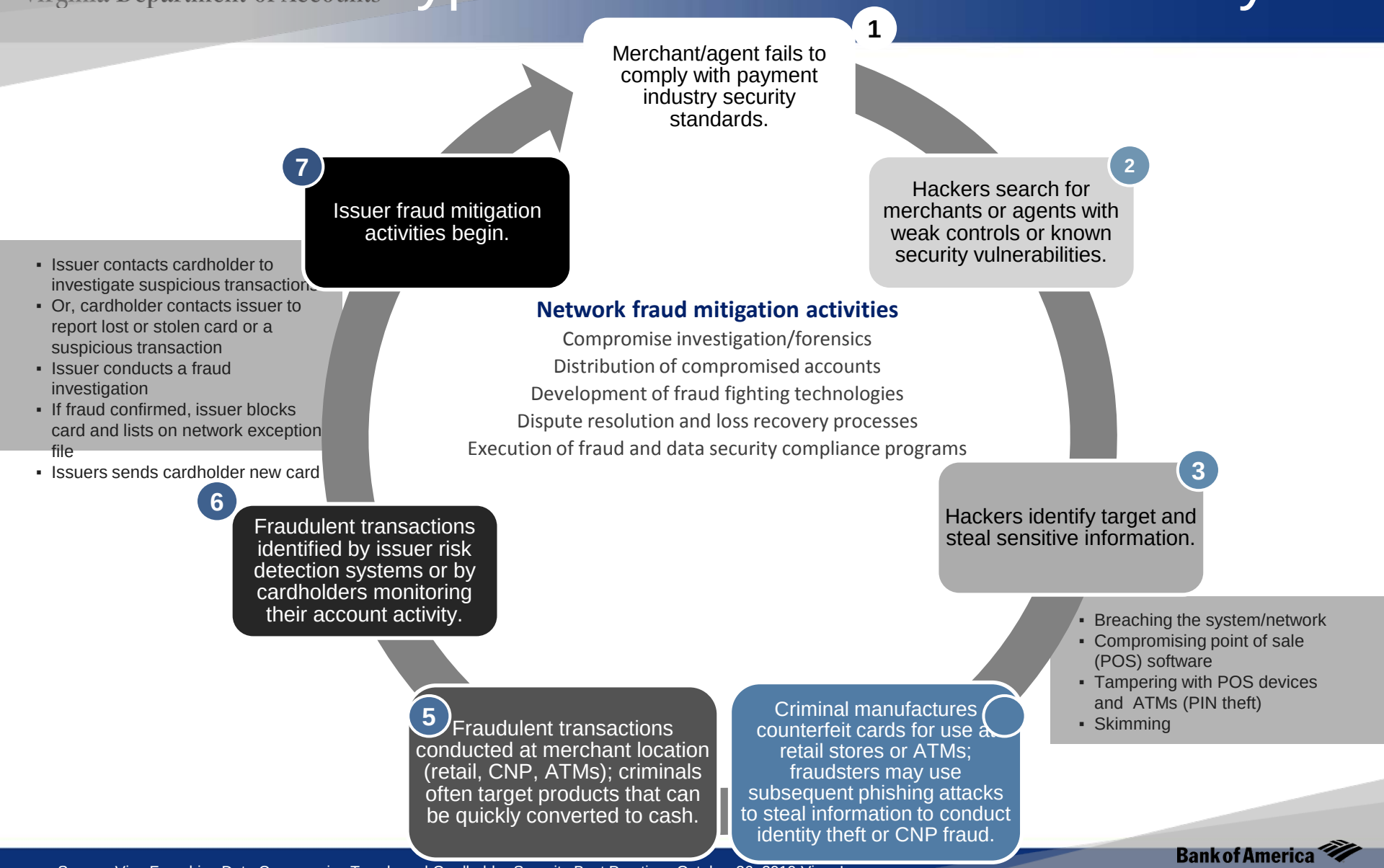
- Receipts- Statement manipulation
- PayPal- Payment to vendor with a personal name instead of business name
- Square- Payment to vendor with a personal name instead of business name
- Level 3 data- Look at payment details

Focused on card fraud prevention

- Fraud trends
  - external
  - internal
- Issues
- Examples

Virginia Department of Accounts

Typical data breach and fraud cycle



Source: Visa Franchise Data Compromise Trends and Cardholder Security Best Practices October 26, 2010 Visa, Inc.

Bank of America Merrill Lynch

Virginia Department of Accounts

Fraud servicing scenarios

Authorizations that need to be validated

- 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 phone attempts can not be made, email sent to primary contacts to ask for a return call

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 will send a fraud statement to the Program Administrator or cardholder via email, fax or regular mail
- Program Administrator or cardholder may be 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
- Once the credit is applied to the account, the claim is resolved

Client action

Call the Fraud department at 866-500-8262 or collect 509-353-6656.

The department is available 24/7 to assist with questions or verification.

The path forward

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

Payment trends and considerations

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

SERVICE QUALITY AWARD WINNERS
Visa 2015, Commercial Credit
Authorization Approval Rate, Domestic & International

#1 IN FRAUD PREVENTION, 10 years in a row
Javelin Research, 2016
10th Annual Credit Card Issuers' Identity Safety Scorecard