Fraud Protection, You and Your Bank

Maximize your chances to minimize your losses

Presentation for Missouri GFOA April 2011

By: Terry Endres, VP, Government Treasury Solutions
Phone: 314-466-6774
Terry.m.endres@baml.com

Bank of America
Merrill Lynch

Know the Code

Revised Articles 3 & 4 of the Uniform Commercial Code (UCC)

- "Ordinary Care" in payment of checks – Banks not required to manually inspect and verify signatures if using automated means and they are similar to other banks
- Comparative Negligence Standard – clients and banks share liability
  - Client's Duty to Discover and Report Unauthorized Signature or Alteration
  - Within a reasonable timeframe – was 14 days, now 30 days
  - Client is absolutely precluded from asserting a claim, without regard to negligence of the bank or the client, if the client does not discover and report within one year after the statement or items are made available

Know the Code

Revised Articles 3 & 4 of the Uniform Commercial Code (UCC)

- **Additional Information on UCC Articles 3 & 4**
- American Law Institute – Individuals can order the most recent edition of the Uniform Commercial Code from their website, www.ali.org or by using this specific URL: http://www.ali.org/ali/com_ucc.htm
- National Conference of Commissioners on Uniform State Laws, http://www.nccusl.org/ has fact sheets on UCC 3 & 4

Legal Disclaimer for Previous Slide

Make sure to have your own opinion on UCC

- *The information provided in this document is of a summary nature and is not designed to replace the guidance of a qualified legal representative who is familiar the UCC in the particular state(s) in which client does business with Bank of America.*
- *Articles 3 and 4 of the UCC are also being looked at for ways they may better reflect the modern processing of banking transactions. The client should be seeking legal advice from the client's own legal adviser.*

Check Fraud – It's a Big Deal!

Source: ABA 2009

- Industry check-related losses amounted to an estimated $1.024 Billion in 2009
- Up from $969 million in 2006
- It's NOT going down!

Check Fraud – How do they do it?

Two Broad Categories:

- Counterfeit: An act of making an imitation check with intent to deceive
- Forgery: An act of altering a check or signature with intent to deceive or of signing another's name to a document with deceitful and fraudulent intent
- In a downward economy, the risk of fraud is even greater

Ounce of Prevention = Big $$$$

According to ABA, 92% of $12.6 billion in attempted fraud in 2006 was caught by banks!

- American Banker Association (ABA) surveys have shown for a number of years that
  - Positive Pay
  - Teller Positive Pay
  - Account Reconcilement Services -- continue to be the most effective check fraud prevention services
- Fill out a Fraud Checklist with your bank
- Additional Fraud Tools:
  - ACH Positive Pay
  - Check stock security features
  - Dollar and date controls
  - Check outsourcing
  - Electronic payments

PCI: Let's start from the beginning…

Payment Card Industry Compliance

- PCI stands for the Payment Card Industry and refers to:
  - The PCI Security Standards Council (PCI SSC), an industry body founded by the major card brands to protect cardholder data. Founders:

  - The global Security Standards created and maintained by the PCI SSC to protect cardholder payment data.

Merchants are Required to Keep Customer Data Safe

- If you accept payments via credit, debit, or prepaid cards, the major card brands – Visa, MasterCard, etc. – require that you protect **cardholder account data** handled by you, or on your behalf by a service provider
- Protecting certain elements of cardholder account data (such as truncating the card's Primary Account Number and Expiration Date on receipts) may also be required by various state laws and federal law
- Additionally, various state and federal laws also contain requirements to protect customer Social Security and other personal data
- Merchants must understand what data security laws and regulations apply to them…and comply!

Inadequate Security Leads to Data Compromise Incidents

What we're preventing

- A data compromise is an incident involving the breach of a system or network where cardholder data is processed, stored or transmitted.
- A data compromise can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data.
- There are the three basic types of data security breaches that can lead to a data compromise:
  - Physical Breach – theft of documents or equipment
  - Electronic Breach – electronic breach of a system or network environment
  - Skimming – capture of card magnetic stripe data using an external device

Reducing the Risk of Compromise via PCI Compliance

Your responsibility

- The major credit card companies, including Visa and MasterCard, require any business which accepts credit, debit, or prepaid card payments to comply with the Payment Card Industry Data Security Standard (PCI DSS)
- The PCI DSS is a global standard for protecting cardholder account information to reduce the risk of data compromise
- The PCI DSS consists of 12, "digital dozen" requirements for protecting card account information, and operates on the following principles:
- If you don't need cardholder account data, don't store it
- Never store sensitive authentication data (i.e. full magnetic card stripe data, card verification values, or PIN/PIN block data), after transaction authorization
  - If you store permitted cardholder account data (i.e. full Primary Account Number, cardholder name, service code, and expiration date), it must be protected in accordance with the PCI DSS "digital dozen" requirements
  - If you use a service provider(s) to handle cardholder account data on your behalf, you must ensure your service provider(s) handles this data in accordance with PCI DSS requirements

A Closer Look at the PCI DSS – Requirements

- All card accepting merchants must comply with all applicable requirements, below.
- Not all PCI DSS requirements apply to all merchants. Merchants must review each requirement to determine applicability to the merchant's card payment acceptance systems and business processes.

Objective	PCI DSS Requirement
Build and Maintain a Secure Network	**1** Install and maintain a firewall configuration to protect cardholder data **2** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3** Protect stored cardholder data **4** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5** Use and regularly update anti-virus software **6** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7** Restrict access to cardholder data by business need-to-know **8** Assign a unique ID to each person with computer access **9** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10** Track and monitor all access to network resources and cardholder data **11** Regularly test security systems and processes
Maintain an Information Security Policy	**12** Maintain a policy that addresses information security

Ounce of Prevention – Best Practices

Are you doing these?

- Reconcile accounts daily
- Segregate duties internally of financial activities (Audit/Control)
- Consider migration from Check to electronic Payment Products
- Become more fraud focused on inquiries from other banks or institutions where questions regarding legitimacy of checks
- Separate Funding Only Accounts on No Check Activity Status to prevent counterfeit item from clearing
- Escalate suspicious activities to client manager team to review with Fraud Monitoring Team

Ounce of Prevention – Electronic Payment Controls

Get rid of the paper

- Direct Deposit Payroll or other payments depositing via ACH (Automated Clearing House)
- ACH Positive Pay Allows review to accept or reject transactions real time
- ACH Blocks and Auths Restrict non-authorized attempts
- Corporate Cards Manages payments associated with purchasing supplies, travel, and vendor payments
- Payroll Card Alternative to Direct Deposit to VISA card for use at POS (Point of Sale) terminals and ATM machines
- Prepaid Card Single use or recurring payment to VISA card

When it happens

DON'T ASSUME THE BANK WILL COVER IT!

- Report it to your bank right away
- Report to local law enforcement
- Make sure to implement the recommended services to prevent it from happening again