Payment Law Update

FedExchange 2010
Springfield, Massachusetts
Patricia Allouise and Lisa Wright
Legal Department
Federal Reserve Bank of Boston

June 3, 2010

Objective

- Review some of the latest payment laws and regulations impacting financial institutions
  - Payments fraud and current events
    - Focus on remotely created checks, electronically created payment orders, and remote deposit capture
    - Focus on corporate account takeovers
  - Payment Law Update “Rapid Fire”
    - Unlawful Internet Gambling
    - Data Security
    - Rule 314(a)
    - Treasury Initiatives
    - Regulation E and certain overdrafts
    - Payment related actions
    - Regulation CC changes
- Question and Answers

Payments Fraud

- 73% of organizations experienced attempted or actual payments fraud in 2009

- 9 out of 10 organizations (90%) that experienced attempted or actual payments fraud in 2009 were victims of check fraud

- Source: 2010 Association for Financial Professionals Payments Fraud and Control Survey Report of Survey Results available at:
  http://www.afponline.org/pub/pdf/2010_Payments_Fraud_Survey.pdf

Payments Fraud (continued)

- Checks remain the payment method most frequently targeted by criminals to commit payments fraud. Among the most widely used techniques to commit payments fraud were:
  - Counterfeit checks using the organization's MICR line data (72%)
  - Alteration of payee names on check issued by the organization (58%)
  - Alteration of dollar amount on checks issued (35%)

FFIEC IT Examination Handbook

- Revision in February 2010 to the Retail Payments Systems Booklet
  - Provides guidance to examiners, financial institutions, and technology service providers on identifying and controlling risks associated with retail payment systems and related banking activities
  - Distinction: Mature payment systems are better understood, whereas emerging payment systems required a closer look to better understand the risks and associated controls

- Available at: http://www.ffiec.gov/ffiecinfobase/booklets/Retail/retail.pdf

FFIEC IT Examination Handbook

- Check-Based Payments
  - Remotely Created Checks
  - Electronically Created Payment Orders
  - Remote Deposit Capture

Remotely Created Checks

- Defined in Regulation CC (229.2(fff)) as “a check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn.”
  - Example: signature line says “Authorized by Drawer”
  - Warranty Shift to the bank of first deposit

Remotely Created Checks

- April 2010: OCC enters into a settlement agreement with T Bank, N.A., Dallas, TX
  - T Bank required to make $5.1 million in restitution to over 60,000 consumer adversely affected by T Bank's relationship with a third party payment processor and several telemarketers and internet merchants
  - T Bank required to pay a $100,000 civil money penalty
  - Practices cited by the OCC in the settlement involved the use of remotely created checks
  - Available at: http://www.occ.treas.gov/ftp/release/2010-45.htm

Electronically Created Payment Orders

- Practice in which a merchant takes payment instructions for goods and services and places them in an electronic template that creates an electronic file for processing through the check clearing networks
  - EPO did not begin with a paper item
  - Implications under Federal Reserve Operating Circular No. 3

Remote Deposit Capture

- Allows for scanned checks to be deposited electronically from the back office of a company to its bank account

- Remember: FFIEC Guidance on Risk Management of Remote Deposit Capture available at: http://www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf

- 2010 AFP Payments Fraud and Control Survey: "Despite the increase in the use of remote deposit, there have been very few incidents of fraud originating from the use of scanned checks. Just three percent of survey respondents whose organizations use remote deposit indicate their organizations were subject to payment fraud originating from the service."

Payments Fraud

Small and midsized businesses and their financial institutions suffered about $120 Million in losses due to fraudulent EFTs in 3Q 2009, up from about $85 Million in 3Q 2007.

Source: David Nelson, Examination Specialist with the FDIC Cyber Fraud and Financial Crimes Section

Available at: http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1411123,00.html

DIs liable for Cyber Crimes?

- If a corporate customer/member's account is hacked and/or account information is otherwise compromised and funds are lost--who is responsible?
- Several corporate customers have sued their DIs alleging the DI is responsible for not protecting the customer's funds from theft (e.g. negligence, breach of contract, breach of fiduciary duty)
- Other corporate customers argue that there is a common law duty to protect customer's confidential information from identity theft
- Many ACH cases are focusing on whether the security procedures in place were "commercially reasonable" UCC §4A-202

Commercially Reasonable

What some plaintiffs have argued is required for their situation:

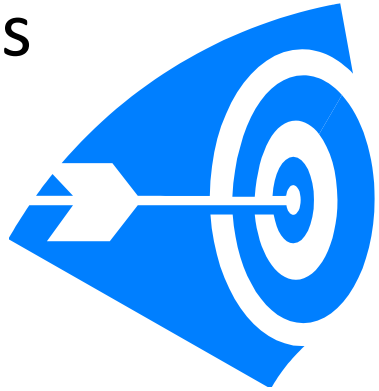
- Multifactor authentication (FFIEC's 2005 "Authentication in an Internet Banking Environment")
- Block of unknown IP addresses
- Red flagging atypical payments
- ACH transfer limits
- Notify via other means (e.g. phone call)
- Dual control option (e.g. transaction origination and authentication)

Regulatory/Legislative Developments

- The FFIEC regulators, lead by the FDIC, are looking back at the 2005 Guidance on Authentication to figure out whether or not the guidance needs updating
  - FDIC held a symposium on Cyber-Related Threats Targeting Small and Midsized Business, “Combating Commercial Payments Fraud,” on May 11
- Multiple bills pending at the federal level trying to address Cyber Security and data privacy

Payment Law Update
"Rapid Fire"

- Unlawful Internet Gambling
- Data Security
- Rule 314(a)
- Treasury Initiatives
- Regulation E and certain overdrafts
- Payment related actions
- Regulation CC changes



Unlawful Internet Gambling Enforcement Act (UIGEA)

- UIGEA prohibits any person engaged in the business of betting or wagering from knowingly accepting payments in connection with the participation of another person in unlawful Internet gambling, known as a "restricted transaction"

- UIGEA required the Board and the Department of the Treasury to identify payment systems that could be use to facilitate such restricted transactions—such a designation makes the payment system, and the financial transaction providers participating in the system, subject to the requirements of the regulations

- The Board labeled the regulations "Regulation GG"

The "Designated Payment Systems"
ACH
Card Systems
Check Collection
Money Transmitting Businesses*
Wire Transfer System

Regulation GG

- One Reg GG obligation was to have designated payment systems develop policies and procedures reasonably designed to identify and block, or otherwise prevent and prohibit, restricted transactions
- Regulation GG provides an exemption to all participants in the ACH systems, Check Collections systems, Wire Transfer systems, and Money Transmitting Businesses, *except* for participants that possess the customer relationship with the commercial recipient of the funds
- Final rules became effective 1/19/2009 with compliance originally required by 12/1/2009
- Compliance was extended on November 27, 2009 to June 1, 2010
- HR 2267 Introduced by Rep. Frank
- Reg GG Available at: http://www.federalreserve.gov/newsevents/press/bcreg/bcreg20081112a1.pdf
- Small Entity Compliance Guide Available at: http://www.federalreserve.gov/bankinforeg/regggcg.htm

Data Security Regulations

- In late 2009, Office of Consumer Affairs and Business Regulations issued the regulations "Standards for the Protection of Personal Information of Residents of the Commonwealth", 201 Code of Massachusetts Regulations 17.00 et seq.
  - Available at: http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

- To Whom does it apply?
  - All natural persons, businesses and other legal entities that own, license, store or maintain personal information about a resident of the Commonwealth, except state agencies

- Personal Information is essentially a Massachusetts resident's first name (or first initial) and last name in combination with:
  - a Social Security number
  - a driver's license number or state-issued identification card number **or**
  - a financial account number

Data Security Regulations

- Requires the development, implementation, maintenance and monitoring of a “written information security program” (WISP)
- Lists minimums that a WISP must include
- Lists minimums for a computer security system
- Effective Date March 1, 2010

FinCEN

The “314(a) Rule”: allows FinCEN to require financial institutions to search their records to determine whether they have maintained an account or conducted a transaction with a person that a law enforcement agency has certified is suspected, based on credible evidence, of engaging in terrorist activity or significant money laundering activities

Rule 314(a) changes

- FinCEN extending the use of the 314(a) program to include foreign law enforcement agencies (EU) and state and local law enforcement agencies
- Clarified that FinCEN, on its own behalf and on the behalf of other entities of the Treasury, may also initiate 314(a) queries
- Final Rule effective February 10, 2010

Treasury Initiatives

- Treasury Initiatives:
  - April 19, 2010 Press Release
    - Require individuals receiving certain benefit payments to receive payments electronically
    - Businesses currently permitted to use paper Federal Tax Deposit coupons will have to make those deposits electronically beginning in 2011 with a few exceptions
    - Available at: http://www.ustreas.gov/press/release/tg644.htm
  - April 19, 2010 Proposed Rule on garnishment of accounts containing federal benefit payments
  - May 14, 2010 Proposed Rule related to ACH

Regulation E and certain overdrafts

- November 2009 – final rule amending Regulation E and the commentary
  - Limits the ability of a financial institution to assess an overdraft fee for paying automated transfer machine (**ATM**) and **one-time debit card transactions** that overdraw a consumer's account unless a consumer affirmatively consents, or **opts in**, to the institution's payment of overdrafts for these transactions
  - Effective date of July 1, 2010 for new account holders and August 15, 2010 for existing account holders

- Proposed rule still pending regarding questions that have arisen and certain technical corrections

Payment related actions

- Payment related actions:
  - Example: Woodforest Bank, Refugio, Texas, agreed to pay a penalty and restitution for overdraft protection program Available at: http://www.ots.treas.gov/?p=PressReleases&ContentRecord_id=2cf1106c-a72d-a2a6-0bb9-0e36dce9351b&ContentType_id=4c12f337-b5b6-4c87-b45c-838958422bf3
  - Example: In Re: Checking Account Overdraft Litigation, S.D. Fla., No. 09-MD-020236 JLK
  - Example: New York Attorney General Andrew Cuomo settlement with Citibank over "free" accounts

    Available at: http://www.ag.ny.gov/media_center/2010/feb/feb01a_10.html

Regulation CC changes

- Effective February 27, 2010: single check-processing region for purposes of Regulation CC
  - No longer any checks that are nonlocal

- Future Changes:
  - Expeditious-return requirement
    - Possibility of amending Reg. CC to provide that a depositary bank that has not agreed to receive returned checks electronically will no longer have the right to expeditious return

Question and Answer Session