Information Security and Money Transmitters: Regulatory Landscape, Best Practices, and Other Considerations

September 21, 2016
Presented By
Adam Fleisher
Agenda and Overview

- What are the Risks?
  - Risks particular to money transmitters?
- Who are the Regulators?
  - A growing role for state money transmission regulators?
- What are the Rules, Best Practices, Guidance?
  - Trends in oversight and enforcement
- What should you be thinking about?
  - For Licensees
  - For Regulators
- Wrap-Up
The Risks
What Can go Wrong?

• Types of “incidents” involving personal information
  • Stolen or lost laptop (or jump drive, or backup tape)
  • The “hack” (unauthorized access to your network system)
  • Inadvertent disclosure (coding error, misdirected email)
  • Newer trends—phishing attacks, ransomware
  • Dumpster diving (improper disposal)

"WE’VE NARROWED OUR SECURITY RISKS DOWN TO THESE TWO GROUPS."
Security Incidents

• Increasing in size and scope
• Affecting companies big and small
  • Home Depot, Target, Anthem, eBay, Adobe, Sony, Schnuck’s, Wendy’s, P.F. Chang’s, Michael’s, and so on.
• New threat vectors/attack methodologies
  • Phishing
• Ramifications
  • Investigation and possible enforcement—multiple regulators
  • Reputational harm
  • Disruption to business
  • Cost
  • Class action liability
• Having a breach has never been less fun!

“I think we’re past the point where rebooting will help.”
Money Transmitters

• Some considerations
  • Distributed networks (agent locations)
  • Multiple customer touchpoints (mobile, POS, etc.)
  • Receiving, holding and transferring consumer funds
  • Collect, use, and store financial account information
  • *Required* to collect and maintain (for up to 5 years) personal information such as name and address *and* sensitive consumer data such as Social Security numbers.
Who are the Regulators?
Federal and State Authorities

- A number of federal and state regulators in the data security space
  - Multiple, overlapping jurisdictional authorities
Federal Regulators

• For years, the Federal Trade Commission has been the most prominent regulator in the data security space
  • Section 5 of the FTC Act prohibits unfair or deceptive acts and practices in or affecting commerce
  • The Gramm Leach Bliley Act (GLBA) Safeguards Rule requires covered financial institutions to develop, implement, and maintain a written comprehensive information security program.

• Two recent players
  • The Consumer Financial Protection Bureau
    • Prohibits covered persons and service providers from committing or engaging in an unfair, deceptive, or abusive act or practice in connection with any transaction with a consumer for a consumer financial product or service or the offering of a consumer financial production or service
  • The Securities and Exchange Commission
    • Statements that could be construed as misleading to investors
State Regulators

• In general, state attorneys general regulate and enforce in the data security space through consumer protection and UDAP laws, similar to Section 5 of the FTC Act
  • State AGs also enforce:
    • Data breach notification laws
    • State laws pertaining to safeguarding and the disposal of sensitive personal information
• State money transmitter regulatory authorities
  • General safety and soundness examination authority
  • Specific regulations and guidance on data security issues
  • Special requirements for licensees that handle virtual currency
Rules, Best Practices, and Guidance
Overview

• Variations on general theme
  • A company must have a written information security program that is “reasonable” and appropriate in light of an entity’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue.

• Relatively few proscriptive, binding laws or rules
  • But some things could be deemed *de facto* unreasonable
  • And trend toward specificity

• A lot of guidance
  • FTC
  • State AGs
  • Banking Departments

• State data breach notification laws and related laws

“That’s our CIO. He’s encrypted for security purposes.”
The FTC – GLBA

- Covered financial institutions must develop a written information security plan that describes their program to protect customer information.

- All programs must be appropriate to the financial institution’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. Covered financial institutions must:
  - Have a designated employee or employees to oversee the program;
  - Identify and assess the risks to customer information and evaluate controls to address these risks;
  - Design an information security program, and detail the plans to monitor it;
  - Select appropriate service providers and require them (by contract) to implement the safeguards; and
  - Evaluate the program and explain adjustments in light of changes to business arrangements or the results of security tests.
The FTC – Section 5

• Section 5 of the FTC Act prohibits “[u]nfair or deceptive acts or practices in or affecting commerce”

• The FTC has used its Section 5 authority to bring enforcement actions related to data security practices about 60 times

• How do deception and unfairness apply to data security incidents?
  • Deceptive statements in public representations, particularly posted privacy policies
    • “We use reasonable security measures…”
    • Any specific representations made about your data security practices
  • Unfair security practices with regard to the treatment of consumers’ personal information
    • The FTC takes the position that there is a duty to protect data implied in the requirement not to engage in unfair practices—a duty to have “reasonable” security measures in place
“Unfairness” – LabMD

• Clinical testing laboratory that tested samples for physicians
  - In May 2008, a LabMD insurance-related report was apparently made available on a peer-to-peer file-sharing network
    - Contained sensitive information
• FTC unfairness test
  - Act or practice must (1) cause or be likely to cause substantial injury to consumers that (2) is not reasonably avoidable by them and (3) is not outweighed by countervailing benefits to consumers or to competition.
• ALJ ruling
  - FTC failed to establish that consumers had suffered, or were likely to suffer, any injury as a result of LabMD’s allegedly unreasonable data security practices
    - Must have some evidence of tangible harm
• Commission ruling
  - LabMD’s data security practices met the first prong of the unfairness test because they both (1) caused substantial injury; and (2) were likely to cause substantial injury.
    - A range of harms that “can and often do” result from unauthorized disclosure of sensitive personal information, including identity theft and medical identity theft.
    - Mere disclosure constitutes a substantial injury because disclosure of sensitive medical information, including tests performed, can “involve ‘embarrassment or other negative outcomes, including reputational harm’
"Reasonableness"

• The FTC’s reasonableness standard
  • Companies that maintain information about consumers should employ reasonable safeguards—*including physical, technical, and administrative safeguards*—to protect that information. The level of security required should *depend on the sensitivity of the data, the size and nature of a company’s business operations, and the types of risks a company faces.*

• Considerable overlap with Safeguards Rule concept
  • When the FTC has brought data security enforcement actions against companies subject to its GLBA jurisdiction, it generally has alleged violations of both GLBA and Section 5.

• The FTC is getting more proscriptive
  • Recent blog post—the NIST Cybersecurity framework is not a safe harbor, but a set of “fundamental security practices”
    • Five functions “signify the key elements of effective cybersecurity”
      • Identify, Protect, Detect, Respond, Recover
  • Can a security program *not* consistent with this framework still be reasonable?
The CFPB – Dwolla

• Last March, the CFPB issued a consent order against Dwolla based on allegations that Dwolla made false representations to consumers regarding its data security practices
  • Dwolla allegedly made broad promises to consumers, such as that “100% of [their] info is encrypted and stored securely” and that the company encrypted all “sensitive information that exists on its servers.”
  • Dwolla allegedly did not live up to these promises. For example, Dwolla allegedly:
    • Did not conduct risk assessments or train its employees regarding security; and
    • Did not in fact use encryption to safeguard sensitive information

• Note, this was UDAAP
  • The CFPB concluded that Dwolla deceived its customers because the representations that the company made regarding its data security practices were “likely to mislead a reasonable consumer” regarding whether Dwolla had incorporated reasonable and appropriate data-security practices
The CFPB – Now What?

• CFPB assessed a civil money penalty of $100,000 against Dwolla, and the company is required to take a wide variety of steps to improve its security practices, in addition to being prohibited from making misrepresentations regarding its security practices.

• The CFPB has placed a stake in the ground
  • The FTC could have brought the same action alleging that Dwolla’s security practices failed to comply with the FTC’s GLBA safeguards rule or that Dwolla’s representations regarding its security were deceptive, in violation of Section 5 of the FTC Act.
  • While the civil money penalty assessed in this case is small compared to other recent CFPB actions (but bigger than the zero dollars the FTC can directly impose for a general violation of Section 5), the consent order is significant because of the CFPB’s contention that its UDAAP authority extends to data security.
The SEC

- A new focus on data security incidents
- Generally speaking, publicly traded companies must consider whether statements regarding an incident could be construed as misleading to investors
  - Also must consider whether an incident is material and requires any notice or other communication
  - Historical statements about data security, including risks, must not be misleading
- SEC may investigate these types of issues in the event of a significant data security incident
States – Generally Applicable Regimes

• Breach Notification: Almost all of the US states require notice to individuals (and many also to regulators)
• More than 30 states have laws relating to SSNs
• State disposal laws
• State data security laws of general applicability (Mass, Nevada)
Massachusetts Regulations

- Risk Assessment
- Written Information Security Program
- Physical Security
- Electronic Security
- Encryption for data in transit across public networks and stored on laptops
- Select and Retain Competent Service Providers
- Employee Training
- Policies regarding storage, access, and transportation of personal information outside of business premises
- Authentication and access controls
- Prevent terminated employees from accessing personal information
- Document response to breach incidents and post-incident review
California AG Guidance

- California Attorney General 2016 Data Breach Report includes guidance on what the AG believes constitutes “reasonable” security for purposes of complying with the California safeguards law.
- A business must “at a minimum” meet the Center for Internet Security’s (CIS) Critical Security Controls. These controls include:
  - Secure configuration
  - Access controls
  - A vulnerability and patch management program
  - Blocking of vulnerable access points
  - Monitoring of accounts and audit logs
  - Protect key assets
  - Security training
  - Testing of defenses
  - Planning and preparing to respond promptly and effectively to security incidents
States – Money Transmission Regimes

- Safety and soundness authority – Examinations
- NYDFS cybersecurity regulations
- Pennsylvania guidance and Washington regulations
- Specific virtual currency focus
On November 9, 2015, the New York Department of Financial Services sent a letter to a number of state and federal agencies signaling that the NYDFS may issue comprehensive cybersecurity regulations for financial institutions subject to the authority of the NYDFS.

Last week, NY DFS issued comprehensive cybersecurity regulations

- Broad definition of covered entity—includes agents?
- Broad definition of covered information
- Cybersecurity program that conducts “core” cybersecurity functions, including identifying risks, developing “defensive infrastructure,” detecting, responding to, and recovering from Cybersecurity Events, and fulfilling regulatory obligations
- Written cybersecurity policy setting forth policies and procedures to protect “Information Systems and Nonpublic Information stored on those Information Systems” and addressing, “at a minimum,” fourteen areas.
• Specific requirements include:
  • Must have a Chief Information Security Officer
  • Annual penetration testing and quarterly vulnerability assessments
  • Audit trail and **detailed and extensive logging**
  • Employ cybersecurity personnel “sufficient to manage” cyber risks, regular training and “steps to stay abreast of changing cybersecurity threats and countermeasures”
  • Procedures and requirements relating to vendors and other third parties
  • **Multi-factor authentication required for any remote access**
  • Risk-based authentication mechanisms for access to web applications that “capture, display, or interface with Nonpublic Information”
  • Training and monitoring
  • **Encryption of all Nonpublic Information in transit and at rest**
  • **Notice of Incidents within 72 hours**—much broader than current general breach **notice requirement**
  • Annual risk assessments
  • Application security for internally developed and third-party applications
  • Incident response plan
• Written certification to compliance
Pennsylvania, Washington

- Pennsylvania DBS cybersecurity letter and guidance (2015)
  - Strongly encourages all of regulated entities to develop cybersecurity attack prevention and mitigation plans. Suggestions include:
    - Identify and assess security risks
    - Evaluate means and methods to protect networks and data
  - Provides resources webpage, including FFIEC, CSBS and FTC information
- Recently amended Washington Money Transmission Act regulations
  - Cybersecurity program—Each licensee shall establish and maintain a cybersecurity program to ensure the availability and functionality of the licensee's electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use, or tampering.
    - Also appears to require compliance with GLBA Safeguards Rule
  - Incorporates by reference general statutory breach notification obligation
    - Also must notify DFI “within forty-five days of a data breach”
  - Business resumption/response and recovery plan
Specifics for Virtual Currency

• NY DFS Virtual Currency
  • Virtual Currency licensing regime includes specific cyber security program requirements
    • Somewhat similar to parts of the newly promulgated draft regulations

• Texas Supervisory Memorandum – 1037
  • License applicants who handle virtual currencies in the course of their money transmission activities must submit a current third party security audit of their relevant computer systems

• CSBS Virtual Currency Framework
  • Recommends cybersecurity audits where necessary
    • Flexibility based on business model and activity levels
  • A cyber security program with policies and procedures
  • Customer notification and reporting requirements for cyber security events
Considerations
What Can Licensees Do?

• Written cybersecurity program, including incident response plan
• Thinking about security and about compliance
• Prevent—and prepare

“I sent my bank details and Social Security number in an e-mail, but I put ‘PRIVATE FINANCIAL INFO’ in the subject line so it should be safe.”
Common Elements on Data Security

- Risk assessment
- Appoint individual(s) to be in charge of security
- Inventory of locations of personal data
- Supervision of service providers

"A hacker broke into our computer system and, in a random act of kindness, organized all of our files."
Common Elements on Data Security

- Conduct training
- Detailed policies for administrative, physical, and technical security measures
  - Basics include
    - Access management
    - Intrusion detection and prevention, and monitoring
    - Network segmentation/defense in depth
    - Heightened protection for sensitive information
    - Vulnerability assessments
    - Patch management
    - Secure paper, physical media, and devices
- Regularly update practices
- Incident Response Plan
What the FTC Looks for: Seven Themes

- What was the nature of the unauthorized access to personal information (or the risk)?
- What was the scope and nature of the personal information involved?
- Was it foreseeable?
- What representations did you make about data security practices?
- What security policies did you have in place?
- What security practices did you have in place?
- How did you respond to the unauthorized access to personal information (or the risk)?
What Can Regulators Do?

- Regulations, guidance, laws?
- Uniformity and clear expectations
- What to look for?
  - Federal banking examiners as guides? The FFIEC handbook?
- Collaborative versus adversarial
- Consider the various models in this space, entities of varying size and sophistication
  - Risk to any one-size-fits-all approach
Wrap Up and Questions

Adam Fleisher
Morrison & Foerster LLP
Washington, DC
(202) 887.8781
afleisher@mofo.com