PRESENTATION

FINANCIAL INSTITUTIONS AND DATA BREACH DILIGENCE

Catherine C. Long
Birmingham, AL

Craig Nazzaro
Atlanta, GA

Steve F. Wood
Nashville, TN

INTRODUCTIONS

- Speaker Introductions
- Panel Topics
- Questions or Comments

PART ONE

Hot Topics: Data Breach and Cybersecurity Litigation

Catherine Crosby Long

Shareholder

Data Breach Litigation by the Numbers

- Case filings were down 25 percent from the preceding year
- Only five percent of publicly reported data breaches lead to litigation
- Cases filed in 2015-16 focused on the medical industry
- Approximately 20 different legal theories were advanced in the past year
- 75 percent of new cases filed include a claim for negligence
- Litigation against financial institutions compromised only three percent of cases filed in the last year

Why are Cases Filed?

- Data breaches are well-publicized
- Companies have no excuse for not taking reasonable measures to protect data they collect
- When a breach occurs, an assessment is immediately performed to determine why it occurred, how quickly it was remedied and what damages were suffered
- A new focus: attack faulty security protocols PLUS a failure to take immediate action to remedy the breach

2016 BREACH CASES AND SETTLEMENTS

- ***Affinity Gaming v. Trustwave Holdings, Inc***., 2:15-CV-02464, D.C. District of Nevada: Following 2013 malicious hacking of payment card systems, Trustwave employees analyzed the casino operator's systems for more than two months in an effort to determine the extent of the breach, find its source and contain it. At the end of the investigation, Trustwave reported malware had been removed. Subsequent penetration testing conducted by Ernst & Young revealed malware was still present, and subsequent investigation revealed hackers continued to infiltrate system while Trustwave's investigation was ongoing.
- **Claims**: Fraudulent inducement, Fraud, Constructive Fraud, Deceptive Trade Practices, Negligence, Negligent Misrepresentation, Breach of Contract, Declaratory Judgment

2016 BREACH CASES AND SETTLEMENTS

- ***Torres v. The Wendy's Company***, 6:16-cv-00210-PGB, Middle District of Florida: Class action complaint alleged Wendy's employed inadequate safety measures and failed to quickly send notice to customers following breach of computers that handled payment processing at approximately 6,000 locations. The complaint asserted "while many retailers, banks and card companies responded to recent breaches by adopting technology that helps make transactions more secure, Wendy's has acknowledged that it did not do so."

2016 BREACH CASES AND SETTLEMENTS

- ***Varela v. Lamps Plus Inc.***, Case No. 5:16-cv-00577, in the U.S. District Court for the Central District of California, Eastern Division – Riverside: On February 11, a phishing attack allegedly compromised the 2015 W-2 data for Lamps Plus company employees. The data hack occurred as an email spoof appearing as an internal communication, with the hacker gaining access to its networks by simply posing as a Lamps Plus employee. Lamps Plus discovered the data breach during an internal audit, as employees began reporting that tax returns had already been filed under their name.
- Varela filed the proposed class action alleging negligence, breach of implied contract, violations of California's consumer records and unfair competition laws, invasion of privacy, and negligent violation of the Fair Credit Reporting Act.

2016 BREACH CASES

- ***In re Home Depot Inc. Customer Data Security Breach Litigation****, U.S. District Court, Northern District of Georgia, No. 14-md-02583* – Settled in March 2013 for $19.5 million
- The home improvement retailer will set up a $13 million fund to reimburse shoppers for out-of-pocket losses, and spend at least $6.5 million to fund 1-1/2 years of cardholder identity protection services.
- Home Depot also agreed to improve data security over a two-year period, and hire a chief information security officer to oversee its progress. It will separately pay legal fees and related costs for affected consumers.
- No admission of liability

2016 BREACH CASES AND SETTLEMENTS

- ***Lewert v. P.F. Chang's China Bistro,* Inc.,** 2016 WL 1459226 (Seventh Circuit, April 14, 2016): Seventh Circuit reversed district court's dismissal of class action complaint, finding time and expense incurred in preventing fraudulent charges before canceling credit card were "concrete and particularized" injuries that could be addressed by a favorable judicial decision.

PART TWO

Enforcement Activity and How to Avoid It

Which Financial Regulators are Taking the Lead in the Cyber Security and Data Breach Space?

Craig Nazzaro

Of Counsel

What Authority Does the CFPB Have?

Supervisory Authority:

- Depository Institutions: Banks and credit unions with total assets over $10 billion, and their affiliates. These entities will receive regular exams.
- Non-depository Institutions – Mortgage companies, payday lenders, private education lenders (regardless of size); as for other nonbank entities, the CFPB generally must first define by rule the "larger participants" within a particular industry before supervising entities that fall within the rule's definition. Examinations are based on the potential risk the companies pose to consumers, including consideration of a company's asset size, volume of consumer financial transactions, extent of other federal and state oversight, and any other factor the CFPB deems relevant (think complaints, lawsuits, media).

Enforcement Authority:

- Dodd-Frank authorizes the CFPB to conduct investigations to determine whether ***any person*** has violated federal consumer financial law – Title X does provide exclusions including depository institutions with $10 billion or fewer in assets, nonfinancial businesses (except to the extent they offer a consumer financial product or service), real estate brokers, auto dealers, and persons subject to securities, insurance and commodities regulation.

CFPB Enforcement

In the Matter of: Dwolla, Inc.

- Brought under CFPB's UDAAP authority
- CFPB Stated "Rather than setting 'a new precedent for the payments industry' as asserted, Dwolla's data security practices in fact fell far short of its claims. Such deception about security and security practices is illegal."
- The CFPB disposed of the marketing violations by mentioning that Dwolla is enjoined from "misrepresenting, or assisting others in misrepresenting, expressly or by implication, the data-security practices implemented," then immediately moves onto a lengthy discussion on how they must change their data protection procedures.

What are the Prudential Regulators Saying

OCC Semiannual Risk Perspective Comments by Thomas J. Curry

- Strategic, underwriting, cybersecurity, compliance and interest rate risks remain the OCC's top supervisory concerns.
- We can't allow the federal banking system to be compromised by hackers or used by criminals or terrorists.

FDIC Strategic Plan 2015-2019

- Cybersecurity is one risk area that will receive particular attention during the next several years. During this period, the FDIC will enhance its IT examination program for insured institutions and major technology service providers and substantially increase the staff resources that are dedicated to that program.
- Routinely conducts IT and operations examinations at FDIC-supervised institutions and technology service providers (TSPs).

Then There is the FTC

- In the CFPB's enforcement action against Dwolla, it is important to note that the FTC could have brought the same action, but instead of using a UDAAP argument, they could have used sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act or a very similar UDAP argument.

FTC's website states:

- The Federal Trade Commission has authority to enforce the law with respect to "financial institutions" that are not covered by the federal banking agencies, the Securities and Exchange Commission, the Commodity Futures Trading Commission and state insurance authorities.
- This is almost entirely a space shared with the CFPB, so why was Dwolla brought by the CFPB and not the FTC?

Most Specific Guidance to Date Comes out of the FFIEC

What is the FFIEC?

- The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles for the federal examination of financial institutions. Council members include federal regulators from the Federal Reserve, FDIC, CFPB, NCUA and the OCC.

They state that institutions should:

- Create a comprehensive approach to maintain the security and resilience of its technology infrastructure including the establishment of a robust cybersecurity framework.
- Establish an enterprise-wide approach to manage cyber risks with a strong cybersecurity culture as its foundation.

Future Role of the "Cybersecurity Tool" in Exams and Enforcement Action

- Last December, the FFIEC published a notice and request for comment on a proposed cybersecurity tool.

- The assessment consists of two parts:
  (1) Inherent Risk Profile
  (2) Cybersecurity Maturity

- Use of the assessment by financial institutions is voluntary. However, if a financial institution has completed an assessment, examiners may ask the financial institution for a copy, as they would for any risk self-assessment performed by the financial institution.

Prudential vs. Consumer Risk Regulation

- The FFIEC is headed down a path of working with the industry to provide regulatory guidance in the data security and cyber security spaces.
- The CFPB's lack of comments or guidance on the issue is concerning.
- Director Cordray has stated consent orders are "intended as guides to all participants in the marketplace to avoid similar violations and make an immediate effort to correct any such improper practices."
- What will not work is a divide in the approach to exams and enforcement between the CFPB and the Prudential Regulators.

PART THREE

Handing Over the Keys to the Kingdom

The New Focus on Vendor Management in Information Security

Steve F. Wood

Co-chair, Business Technology Group

Chief Information Security Officer

A Note About Perspective

This presentation approaches the topic of vendor management from the perspective of the customer. Certainly a vendor would be well-advised to consider how much data breach risk the contract allocates and what information security obligations it imposes, but in the emerging new world of cyber risk, negotiations over these considerations largely will be at the margins, not over fundamentals.

Customers, especially in the financial services sector, have limited leeway to accept risk that really is in the vendor's control. Accepting cyber risk and information security obligations in customer contracts has become a fact of life and a cost of doing business for vendors.

The good news for vendors is that, at the end of the day, their interests are aligned with those of the customer in seeking to avoid data breaches, and to a significant extent those risks can be mitigated through an effective information security management program.

Axiom

Like a chain, an information security management system is only as strong as its weakest link.

Bad guys in the cyber world are so pervasive and so persistent that any vulnerability will be exploited; it's just a matter of how long before it occurs.

Corollary

All the firewalls, encryption, policies, training and other information security safeguards in the world won't prevent a breach of data that is outside your control.

In assessing the security of your information, it is critical to account for the information security safeguards (or lack thereof) maintained by your vendors having possession of or access to the information.

What is Driving the Focus on Vendor Management?

- Awareness/media – Target (2013) and Home Depot (2014) data breaches were caused by vendors
- Boards of directors – worried about liability
- Senior executives – worried about being fired
- Cyber insurance carriers – worried about exposure
- Regulators – worried about financial system stability and the protection of consumers

Everyone is realizing that vendors can represent the weak link in a company's information security management program.

Regulatory Environment

- CFPB, FFIEC OCC, FDIC, SEC, CFTC, FINRA, FTC, and more all weighing in
- New York State Department of Financial Services proposed vendor requirements reflect emerging best practices:
  - encryption of data in transit and at rest
  - multifactor authentication for access to systems
  - representations and warranties concerning information security
  - right for financial institution to perform cyber security audits
  - notice of cyber security incidents
  - indemnification for data breach losses and costs

Scope of Concern

- Wide range of vendors with possession of or access to information:
  - Hosted software application (SaaS) vendors
  - Data centers and cloud-based infrastructure vendors
  - Managed infrastructure services vendors
  - IT and software application support vendors
  - Security consultants
  - Law firms
- Variety of types of information at risk:
  - Sensitive personal information (financial, health, etc.)
  - Trade secrets (business plans, etc.)
  - Competitively sensitive info (earnings, merger discussions, etc.)

Four Stages of Vendor Management

- Historically, vendor management was focused on operational outcomes, the ability of the vendor to deliver the good or services
- Now companies also must focus on information security risk, the ability of the vendor to safeguard information or access to information
- Vendor management starts before the relationship and continues afterward, in four stages:
  - Due diligence
  - Contracting
  - Monitoring
  - Post-termination

Due Diligence – Questions, Questions, Questions

- How will information be stored, managed, protected, and ultimately returned or destroyed?
- Where will data reside? Who will have access? How is access granted and revoked?
- What technology will be used by the vendor, and has it been evaluated for vulnerabilities?
- Will the vendor use subcontractors? How have they been vetted?
- Are there independent reviews of the vendor's environment?
- Any history of data breach?
- Does the vendor have the financial wherewithal to pay damages for a data breach? What about cyber insurance?
- How would the vendor’s failure affect our business continuity?

Due Diligence – Discovery and Risk Assessment

- Questionnaire
  - For instance, the BITS Shared Assessments Program Standardized Information Gathering (SIG) questionnaire
  - *Questionnaires don't work if the responses are not reviewed by someone knowledgeable in the field.*
- Third-party assurance
  - SOC 1 (SSAE 16) ≠ SOC 2 (AT 101) HINT: You want SOC2
  - ISO 27001 certification
  - *Third-party reports don't work if they are not reviewed by someone knowledgeable in the field.*
- If relying on vendor's cyber insurance to pay for data breach, consider having the policy reviewed by counsel.

Contracting – Key Provisions

- Confidentiality:
  - Customary prohibition on unauthorized disclose or use of info
- Safeguards:
  - Maintain **administrative, physical and technical** safeguards that **reasonably and appropriately** protect the **confidentiality, availability and integrity** of info.
  - Consider specific safeguard requirements, but that specificity can be risky, both legally and practically.
- Downstream restrictions:
  - Either prohibit subcontractors (often not practicable) or require flow-down of information security obligations; consider approval right over subcontractors.

Contracting – Key Provisions (cont'd)

- Data breach:
  - Notice – report *suspected or actual* data breach very quickly (a few hours to a couple of business days)
  - Cooperation – full transparency; cooperate and assist with investigation, notifications, etc.
  - Mitigation – mitigate, to the extent practicable, any harmful effect of a data breach
  - Reimbursement – pay for costs of investigation, notification, credit monitoring, etc.
- Security incident:
  - Notice – report incidents that threatened info even if no data breach (within ten to 30 days; *immediate notice not necessary*)

Contracting – Key Provisions (cont'd)

- Monitoring:
  - Questionnaires – provide accurate and complete written responses to questionnaires regarding vendor's internal practices, books, and records relating to the safeguarding of info and compliance with security obligations
  - Third-party assurance – SOC 2 reports, ISO 27001 certificates, etc.; material breach if any material test exceptions in report or for failure to comply with applicable standards of certification
  - Inspections – make internal practices, books, and records relating to the safeguarding of info and compliance with security obligations available for inspection by customer or its designee
  - Disclaimer – no defense for customer's review (or not) of reports, conduct (or not) of inspections, or failure to detect (or detection of but failure to act on) deficiencies

Contracting – Key Provisions (cont'd)

- Data breach indemnification:
  - Scope – third-party claims vs. first-party costs and losses
  - Triggers – any data breach regardless of fault? data breach arising from breach of security obligations? negligence? gross negligence?
  - Limits – indemnification subject to or excluded from liability cap under agreement? separate higher limitation of liability?
- Cyber insurance:
  - First party vs. third party coverage
  - Exclusions, exclusions, exclusions
  - Problem with additional insured provision
- Return or destroy info at termination of agreement; certify in writing

Monitoring

- Periodic reports (SOC 2, etc.):
  - Won't help (and can hurt) if reports go directly to file; important for someone knowledgeable to read them and act on issues
- Changes that can affect the security equation (risk analysis required):
  - Changes in scope of services
  - Changes in conditions
  - Regulatory changes
- Incident response:
  - Hope a data breach never happens, but be ready if it does
  - Vendor management program must integrate tightly with security incident response plan

Post-termination

- Return or destroy:
  - Most overlooked aspect of vendor management
  - Huge risk in legacy data laying around all over the place
  - Always get certification from vendor that info was destroyed in a secure manner
- Institutionalize lessons learned
  - About the vendor
  - About the process

Other Takeaways

- Context matters (i.e., conduct a realistic risk analysis):
  - Possession of data or persistent access vs. occasional access
  - Degree of sensitivity – data classification is key
  - Amount – impact of data breach is proportional to number of records
- Preach minimum necessary:
  - Does the vendor *really* need all the info?
  - For how long does the vendor *really* need it?
- Beware when requiring disclosure of vendor's security info:
  - Controversial topic, but security policies *really* should not leave the building, as they can create a roadmap for bad guys
  - Consider on-site inspection of security protocols rather than having vendor send copies for review

QUESTIONS OR COMMENTS?

CONTACT INFORMATION

Catherine Crosby Long
Birmingham, AL
clong@bakerdonelson.com

Craig Nazzaro
Atlanta, GA
cnazzaro@bakerdonelson.com

Steve F. Wood
Nashville, TN
sfwood@bakerdonelson.com