Data Breach Hot Topics: Financial Institutions

Presented by:

Paige Boshell and Erin Illman

Bradley Arant Boult Cummings LLP

August 17, 2016

My Background

Paige Boshell

- Team Leader, Cybersecurity and Privacy Team
- Partner, Birmingham Office
- www.bradley.com/practices-and-industries/practices/cybersecurity-and-privacy

Bradley

My Background

Erin Illman

- Member, Cybersecurity and Privacy Team
- Attorney, Charlotte Office
- CA and NC licensed attorney with 10+ years' experience working in San Francisco and Silicon Valley for technology and financial services clients

Bradley

Agenda

- CFPB enforcement, Dwolla and UDAAP
- Vendor management and contracting
- New FFIEC mobile device guidance

Bradley

CFPB Enforcement - Dwolla

Who: Online consumer payment processor

What: Promised that data security exceeded industry security standards and that consumer information was "securely encrypted" or stored.

Failure: Did not use "reasonable" security measures and did not encrypt all private information or test apps accessing it.

Note: No security breach claimed.

CFPB Enforcement - Dwolla

Authority: UDAAP

Violation: Deceptive trade practice - misrepresenting security

Bradley

CFPB Enforcement - Dwolla

Result:

- Consent order requiring $100,000 penalty plus adoption of reasonable security practices

Required:

- Comprehensive data security measures and policies, including risk assessments and audits
- Employee training on these polices and how to protect consumer information
- Investigate and fix security flaws, including web and mobile apps and storage and transmission of data

CFPB Enforcement - Dwolla

What's new:

- First data security action by CFPB under UDAAP
- Consistent with FTC enforcement: trend from deception towards concept of reasonable security

Bradley

CFPB Enforcement - Dwolla

Practice pointers:

- Make sure that disclosed security practices are accurate and complete
- "Reasonable" security: implementation, maintenance and monitoring/testing of IS; encryption of sensitive data during storage and transmission; alliance with industry standards and practices, as well as regulatory requirements; assessment, audit and correction of IS; employee training

Bradley

Vendor Management

- *Regulatory requirement:* The various banking agencies, individually and collectively, require that banks strengthen VM practices with respect to vendor selection, due diligence, contract content and continuous monitoring.
- *Testing tool:* FFIEC cybersecurity assessment tool offers a specific process and ways to measure the quality of VM.
- *Premise:* Banks are liable for certain vendor failures and must fully vet and oversee vendors, based on their risk assessment of the product or service and vendor at issue.

Vendor Management

Specific requirements:

- Board approval and annual review of "significant" vendors, with additional reviews of relationships and contracts upon "material change"
- Periodic management review vendor's operations for compliance with contracts and regulations
- Risk and compliance management of compliance with state and federal law and Bank's internal policies

Bradley

Vendor Management

Specific requirements (cont'd):

- Management oversight and staffing, as well as coordination of various departments through centralized function
- Monitoring of vendor service quality, risk management process, financial condition
- Documentation and remediation of deficiencies

Bradley

Vendor Cyber RM

- *Inventory and classify sensitive information*: crown jewels, assess risk
- *Identify vendor access points, assess risk*
- *Identify permitted vendor uses, assess risk*
- *Evaluate vendor IS, bank policies, assess risk*
- *Consider coordination and interface of IS*

Bradley

Vendor Contracting - Covenants

- *Minimum standards:* Clear and complete statement of performance standards and functional specifications, including confidentiality and security
- *Consumer complaints:* Allocation of responsibilities
- *Regulatory compliance:* Compliance with all laws applicable to bank and/or services (not just vendor) (consider specific flowdowns as part of minimum standards)

Vendor Contracting - Monitoring

- *Ongoing:* Address mechanism for real-time oversight
- *Periodic:* Provide for regular reporting
- *Audits:* Address need for bank audits, audits by third parties, audit standards and certification (SOC-2, PCI), testing (penetration)
- *Coordination:* Provide for coordination of testing with Bank (data breach, business continuity)

Bradley

Vendor Contracting - Negative Covenants

- *Subcontractors:* Consider oversight, due diligence, approval, notice, prohibition, specific flowdowns, ndas

- *Offshoring:* Consider limits or prohibitions when crown jewels are accessible, stored or used or disclosed

Bradley

Vendor Contracting - Remediation

- *Breach:* Consider SLAs, allocation of credits, turnaround times, escalation of dispute
- *Indemnity:* Address vendor liability and indemnity for failures
- *Insurance:* Provide for insurance coverages, consider cyber
- *Termination:* Provide for suspension or termination, transition assistance, minimal disruption

Bradley

Vendor Contracting - Practice pointers

- *Separate confidentiality and security requirements:* Basic standards and additional requirements due to RM, limits on access, use and disclosure, injunctive relief, industry standards, Dwolla
- *Ownership of data:* Ownership and right to request immediate return and/or certification of destruction, limits on retention
- You are only as strong as your weakest vendor

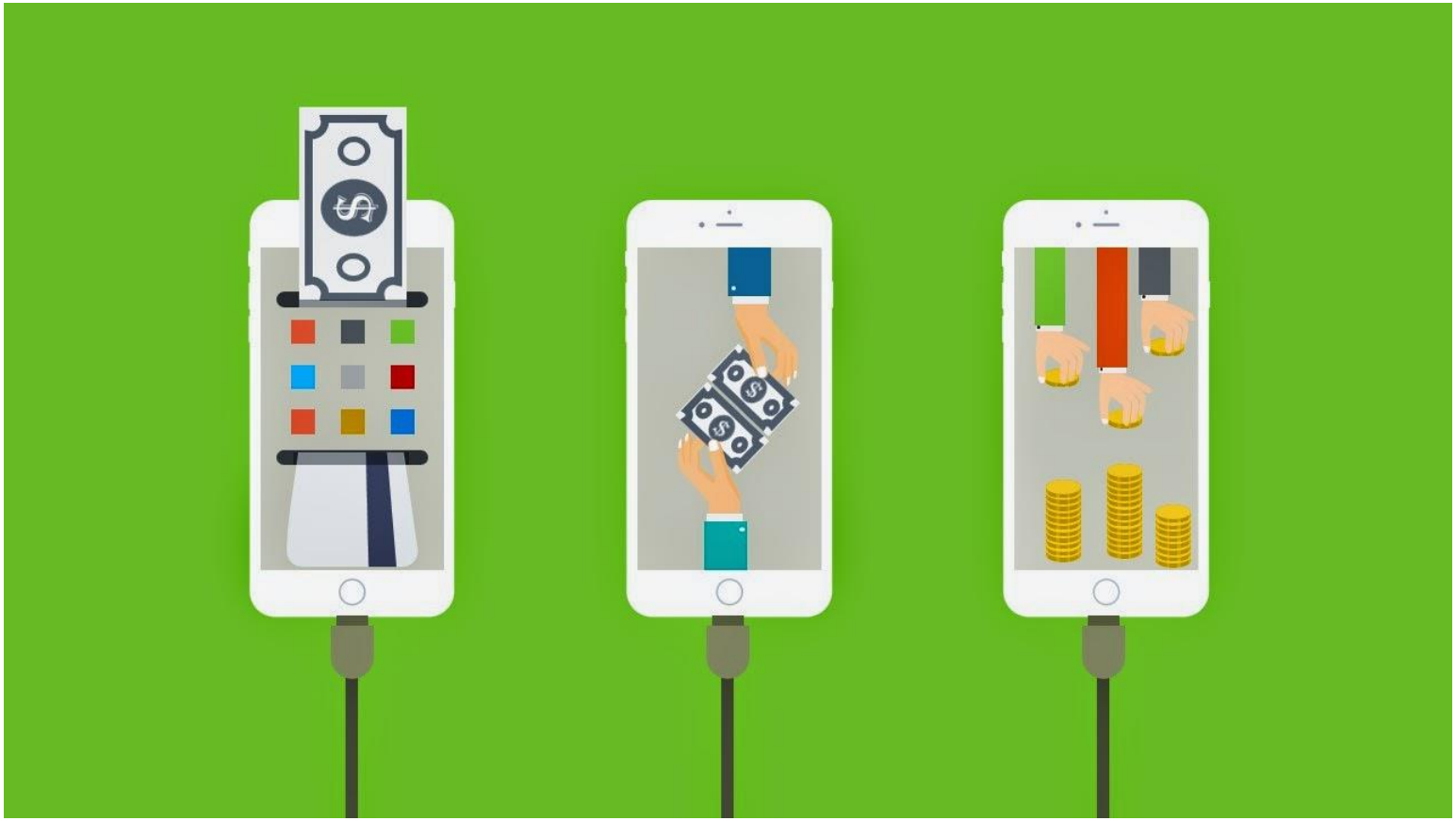
Bradley

Vendor Contracting - Practice pointers

- *Cyberinsurance:* Consider coverages specific to remedies and dependent on financial security of vendor and sensitivity and access/use/disclosure of information
- *Data breaches:* Include separate notice, reasonable assistance and indemnification terms, consider all costs, liability for causing v. failure to prevent

Bradley

Guidance on Mobile Financial Services



Bradley

The Future is Here—Millennials

- 75% of Millennials are at least “somewhat reliant” on a mobile banking application, while more than 25% are “completely reliant”
- 82% of Millennials agree that its beneficial for banks to offer mobile banking
- Nearly half of Millennials want to receive SMS alerts from their bank
- 28% of Millennials would prefer push notifications over SMS alerts
- Nearly 25% of Millennials cite lack of a mobile application as the main barrier to bank engagement

Data from Salesforce Report: 2016 Special Report: What Millennials Expect from Their Banks

Federal Financial Institutions Examination Council (FFIEC)

- FFIEC issued Appendix E, an18 page guidance in April 2016 to address Mobile Financial Services (MFS)
- Appendix E focuses on areas of risk associated with MFS and emphasizes an enterprise-wide risk management approach to effectively manage those risks
- MFS poses special risks relating to device security, authentication, data security, application security, data transmission security, compliance, and third party management

Federal Financial Institutions Examination Council (FFIEC)

- Risk Area:
  - Mobile Financial Services Technologies
- Types of Technologies
  - SMS
    - Text messaging used to provide information to customer, account alerts, or password authentication
  - Mobile-Enabled Web Sites
  - Mobile Applications
    - Downloadable software application, which often involves third party service providers
  - Wireless Payment Technologies
    - POS (point of sale); P2P (person to person), wireless payments

Federal Financial Institutions Examination Council (FFIEC)

- Risk Identification
  - Strategic Risk
  - Operational Risk
    - SMS
    - Mobile-Enabled Web Site
    - Mobile Application
    - Mobile Payment
  - Compliance Risk
  - Reputation Risk

Bradley

Federal Financial Institutions Examination Council (FFIEC)

- Risk Measurement
- Risk Mitigation
  - Strategic
  - Operational
- Monitoring and Reporting

Paige Boshell

pboshell@Bradley.com

205-521-8639

Erin Illman

eillman@Bradley.com

704-338-6026

Christy Roach

croach@Bradley.com

205-521-8610

Bradley