PRE-CON WORKSHOP #3

New FTC Cybersecurity Requirements

What Will Your Auditors Be Looking For?

Michelle Donovan
Partner
Duane Morris

Jessica High
Associate
Duane Morris

Ryan Malouf
Audit Partner
Almich & Associates

CAPPS 39th ANNUAL CONFERENCE
IT STARTS WITH US

"It's better to look ahead and prepare than to look back and regret." – Jackie Joyner-Kersee

GLBA and Safeguards Rule Background

GLBA Components

- Privacy Rule
- Safeguards Rule
  - **Effective June 9, 2023**

GLBA and Title IV

- Program Participation Agreement
- Student Internet Gateway Enrollment Agreement
  - Added requirement of reporting to the Department unauthorized use
- Non-compliance could be determined a lack of administrative capability

Safeguards Rule

What applies as of June 9, 2023

Designated Qualified Individual

Element 1

- Designate a single, qualified individual responsible for overseeing and implementing information security program
- Can be an employee of an affiliate or service provider
- For service providers:
  - Requires designation of a senior person who will be responsible for direction and oversight of the Qualified Individual
  - Requires affiliate or service provider to have an information security program that meets the requirements of the Rule
  - Company retains responsibility for compliance with the Rule

Written Assessments and Polices

- Written Risk Assessment **Element 2**
  - Include criteria for evaluation
  - Identify risks
  - Describe how company will mitigate or accept those risks
  - Must periodically reassess
- Written Information Security Program **Element 3**
  - Based on a risk assessment
  - 8 Controls +
- Written Incident Response Plan

Security Controls – 8+

1. Access Controls – limit to authorized individuals
   - Technical and physical controls
   - Authorized users
   - Only to the extent needed to perform their duties and functions
   - Customer to the extent needed to access their own information
2. Inventory and manage data, devices, systems, facilities
3. Encryption – in transit and at rest
4. Evaluating, assessing or testing third party software
5. Multi-Factor Authentication
6. Data retention policy and procedure
7. Procedures for change management
8. Monitor and log authorized users for any unauthorized access, use or tampering

Security Controls – MFA

- For any individual (employee, customer or otherwise) accessing customer information or internal networks that contain customer information
- Supplement user name and password login with a one-time code generated or received by a device that only the user possesses
  - Digikey
  - Authentication software (Duo)
  - Text may not be sufficient
- Biometric – proceed with caution

Data Retention

- Adopt data retention policy to securely dispose of customer data after 2 years unless it is necessary for:
  - Necessary for business operations
  - Legitimate business purpose
  - Required by law
- Review policies periodically to minimize the unnecessary retention of data

Testing Effectiveness of Controls

Element 4

- Effectiveness of the information security program must be tested through:
  - Continuous monitoring OR
  - Annual penetration testing AND
  - Vulnerability Assessment:
    - At least twice a year
    - Any material change to operations or business
    - Any circumstances arise that materially impact security program

Policies and procedures to ensure personnel able to enact program

Element 5

Ensure that personnel are able to enact the information security:

- Security awareness training updated to reflect risk identified in risk assessment
- Utilize qualified personnel to manage security risks and oversee information security program
- Provide and require ongoing training for security personnel and verify they are taking steps to stay current on emerging threats and countermeasures

Service Providers

Element 6

- Assess service providers to ensure capable of maintaining safeguards
- Contract requirements to implement and maintain safeguards
- Periodically assess service providers based on risk they present and continued adequacy of their safeguards
- See also 8+ control: Element Evaluate, assess, and test third party software applications

Periodic Assessments

Element 7

Periodically evaluate and adjust program based on:

- Results of testing and monitoring
- Any material changes to operations or business arrangements
- Results of the required risk assessments; or
- Any other circumstances that may have a material impact

Incident Response and Reporting

- Establish Incident Response Plan
  - Goals of plan
  - Internal processes for responding to security event
  - Clear definition of roles
  - External and internal communication
  - Requirements for remediation
  - Documentation and report security events
  - Evaluation and revision to response plan following security event
- Qualified Individual must submit an annual, written report to the Board
  - Overall status of the information security program and compliance with Safeguards Rule
  - Material matters such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program

Limited Exceptions < 5,000 Customers

- Not required:
  - Written risk assessment
  - Continuous monitoring or penetration testing (general testing/monitoring still required)
  - Written incident response plan
  - Written annual report by Qualified Individual
- ALL OTHER REQUIREMENTS STILL APPLY

March 2023 Audit Guide

CAPPS 39th ANNUAL CONFERENCE

IT STARTS WITH US

Audit Guide

- Information Security Program must include 7 elements:
- Element 1: Designates a qualified individual responsible for overseeing and implementing the school's or servicer's information security program and enforcing the information security program (16 C.F.R. 314.4(a)).
- If the designated individual is employed by a servicer, determine whether the school:
  - Retains responsibility for compliance with the Safeguards Rule;
  - Designates a senior member of the school's personnel responsible for direction and oversight of the individual; and
  - Requires the servicer maintain an information security program that protects the school in accordance with the requirements of the Safeguards Rule.

Audit Guide

- Element 2: Provides for the information security program to be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks (16 C.F.R. 314.4(b)).
- Element 3: Provides for the design and implementation of safeguards to control the risks the school or servicer identifies through its risk assessment (16 C.F.R. 314.4(c)). At a minimum, the written information security program must address the implementation of the minimum safeguards identified in 16 C.F.R. 314.4(c)(1) through (8).
- Element 4: Provides for the school or servicer to regularly test or otherwise monitor the effectiveness of the safeguards it has implemented (16 C.F.R. 314.4(d)).

Audit Guide

- Element 5: Provides for the implementation of policies and procedures to ensure that personnel are able to enact the information security program (16 C.F.R. 314.4(e)).
- Element 6: Addresses how the school or servicer will oversee its information system service providers (16 C.F.R. 314.4(f)).
- Element 7: Provides for the evaluation and adjustment of its information security program in light of the results of the required testing and monitoring; any material changes to its operations or business arrangements; the results of the required risk assessments; or any other circumstances that it knows or has reason to know may have a material impact the information security program (16 C.F.R. 314.4(g)).

Good News (for now)

- Procedures for this year – **verify**
- There is currently no requirement for an auditor to **test** the effectiveness of an institution's ISP or the institution's compliance with the provisions outlined in its ISP.
- Nor is there a requirement for an auditor to assess the **adequacy** of ISP provisions.

Requirement – Qualified Individual

- **Verify** that the school has designated an individual to oversee, implement, and enforce its information security program.
- If the designated individual is employed by a third party (servicer), determine whether the school:
  - Retains responsibility for compliance with the Safeguards Rule
  - Designates a senior member of the school's personnel responsible for direction and oversight of the individual; and
  - Requires the servicer maintain an information security program that protects the school in accordance with the requirements of the Safeguards Rule.

Recommendation - Qualified Individual

- Formalize designated individual role
  - How is this documented?
    - Job description
    - Memo
    - Board minutes
- If qualified individual leaves be sure that this responsibility is immediately designated to a new team member and document that reassignment of responsibility accordingly
- If using a servicer

Requirement – Information Security Program

- **Verify** that the institution has a written information security program and that the information security program addresses Elements 2-7
- The effective date of an institution's compliance with the information security program requirements is June 9, 2023
- Failure of an institution to design and implement the ISP before 6/9/23 will result in a finding
- CAP for this finding can state the date in which the program was formalized/implemented (subsequent to 6/9 but before the institution's fiscal year end) or where the institution may currently stand in its formalization process

Recommendation - Information Security Program

- Implement written information security program before year end if not currently in place
- Cover policy addressing each of the 7 elements referenced in the Audit Guide
- A good roadmap which identifies how the specific ISP provisions address each of the Elements will greatly help your auditor through this process
- Avoid the need to explain or justify how it “believes” the ISP addresses Elements 2-7 to its auditor.
- Avoid future looking statements of how it “will implement” policies

Audit High Risk Situations

- No designated individual
- No written information security program
- Program does not address 7 elements
- Program not in place by June 9, 2023
- Program not in place by December 31, 2023 with CAP

Anticipating Additional Guidance - Testing

- Audit firms are anticipating additional guidance to come from ED with regard to prescribed testing procedures
- Not just looking for written documentation but also testing whether the program and policies have been implemented and the effectiveness of the program
- This year is a good time for auditors to gain an understanding of an institution's ISP and discuss the various aspects of it with institution personnel
- Auditors can share their professional opinion and thoughts surrounding the plan in light of their anticipated testing of such in the future

USDE Enforcement

Electronic Announcement (Feb 2023)

- Finding of non-compliance (audit or other means) will be resolved by USDE as part of its final determination of an institution's administrative capability.
- No breach = provide a Corrective Action Plan (CAP) with timeframes for coming into compliance with the Rule.
- Repeated non-compliance may result in an administrative action impacting Title IV participation
- If there is a substantial security threat, USDE may temporarily or permanently disable access to Federal Student Aid Application Systems.

Results of Audit Findings

- Referral to the FTC for enforcement
- FSA's Cybersecurity Team will be informed of the GLBA audit findings and may request additional information to assess the level of risk to student data
  - The Cybersecurity Team may provide technical assistance to remediate the security threat, as appropriate
  - If the Cybersecurity Team determines the institution poses a substantial security threat, it may temporarily or permanently disable the school's access to Federal Student Aid Application Systems

FTC Enforcement

FTC Enforcement – FTC Act

- Injunctive Relief
- Civil Penalties - $50,120 per violation, calculated on a daily bases for continuous violations
- Officers can be individually liable if directly participate or have authority to control non-compliance
- Consent Orders
- Severe penalties for violating consent orders
  - Lifelock: company, CEO and COO - 100 Million Settlement for Violation

What to Expect Going Forward

Campus Cyber Security Program

- Details not published
- Last report – data gather phase
- Expect:
  - Amendment to PPA
  - Continued compliance with GLBA
  - CUI Protection
    - NIST 800-171 Compliance Audit
    - NIST 800-171 Self Assessment or Third Party Certification

Security Controls – NIST 800-171

- 2016 Dear Colleague Letter GEN 16-12
  - The Department strongly encourages schools to review and understand the standards defined in NIST SP 800-171
  - The Department strongly encourages those institutions that fall short of NIST standards to assess their current gaps and immediately begin to design and implement plans in order to close those gaps using the NIST standards as a model
- 2020 Department announces a Campus Cybersecurity Program framework for compliance with NIST SP 800-171
- 2021 FSA Conference – still developing framework but schools should be preparing for NIST compliance
- Amendment to PPA expected

Best Practices

- Hire qualified individuals
- Implement security controls set forth in the Rule – not a checklist
- Work on implementing NIST 800-171
- Document policies **and** how policies are implemented
- Conduct and draft written risk assessment – consider counsel for first assessment
- Table top and draft incident response plan
- Diligence and contract review for services providers

Thank You!

- **Michelle Donovan**
  - Partner, Duane Morris LLP
  - 619-744-2219; MHDonovan@duanemorris.com
- **Jessica High**
  - Associate, Duane Morris LLP
  - 619-744-2214; JHigh@duanemorris.com
- **Ryan Malouf**
  - Audit Partner, Almich & Associates
  - 949-600-7550; Ryan@almichcap.com