OFFICE OF THE INSPECTOR GENERAL

U.S. Department of Education

Technology Crimes Division

Cyber Security For Title IV Schools

How Being A “Financial Institution” Changes The Paradigm

Thomas Harper
Assistant Special Agent in Charge
Technology Crimes Division

Agenda

- Who/What is an OIG?
- Department determinations
- GLBA
- Regulatory Authority over Federal Student Aid programs
- Relevant Department of ED communications to schools participating in student aid programs
- Reporting requirements for suspicious events
- Suggestions For Reducing your exposure

What is an OIG?

- Independent component of Federal agencies created by Congress
- Reports to Head of the Agency and Congress
- Inspector General appointed by the President and confirmed by the Senate
- An OIG's mission, generally: to audit and investigate agency programs and operations, promote economy, efficiency and effectiveness, and prevent and detect fraud and abuse

Technology Crimes Division

- Investigate crimes and criminal cyber threats against the Department's IT infrastructure, or
- Criminal activity in cyber space that threatens the Department's administration of Federal education assistance funds
  - Investigative jurisdiction encompasses any IT system used in the administration of Federal money originating from the Department of Education.

Case Examples

- Grade hacking
- Computer Intrusions
- Criminal Forums online selling malware
- ID/Credential theft to hijack Student Aid applications
- Misuse of Department systems to obtain personal information
- Falsifying student aid applications by U.S. government employees
- Child Exploitation material trafficking

Department Determinations

- Educational entities who participate in Federal Title IV Educational Assistance Programs are “financial institutions” and subject to the Gramm-Leach-Bliley Act (GLBA)
  - 12 U.S. Code § 1843(k)(4)(A) - Activities that are financial in nature.
    - “Lending, exchanging, transferring, investing for others, or safeguarding money or securities.”
  - 16 CFR § 313.3(k)(2)(vi) - Examples of financial institution.
    - “A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act and regularly providing that service demonstrates that the business is significantly engaged in that activity.”

GLBA

- Financial Institutions are subject to the data security provisions of the Gramm-Leach-Bliley Act (GLBA) - 15 U.S. Code § 6801-6809
  - "It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."

GLBA

- 16 CFR Part 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION
  - Purpose and Scope
    - implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act (GLBA) and sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

GLBA

- 16 CFR Part 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION
  - Information security program objectives
    - Insure the security and confidentiality of customer information
    - Protect against any anticipated threats or hazards to the security or integrity of such information; and
    - Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

GLBA

- 16 CFR Part 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION
  - Elements
  - In order to develop, implement, and maintain your information security program, *you shall*:
    - (a) Designate an employee or employees to coordinate your information security program;

GLBA

- 16 CFR Part 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION
  - Elements
    - In order to develop, implement, and maintain your information security program, *you shall*:
      - (b) Identify 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 assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
        - (1) Employee training and management;
        - (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
        - (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

GLBA

- 16 CFR Part 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION
  - Elements (cont'd)
    - In order to develop, implement, and maintain your information security program, *you shall*:
      - (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
      - (d) Oversee service providers, by:
        - (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
        - (2) Requiring your service providers by contract to implement and maintain such safeguards.

GLBA

- 16 CFR Part 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION
  - Elements (cont'd)
    - In order to develop, implement, and maintain your information security program, *you shall*:
      - (e) Evaluate and adjust your information security program in light of
        - the results of the testing and monitoring required by paragraph (c) of this section;
        - any material changes to your operations or business arrangements; or
        - any other circumstances that you know or have reason to know may have a material impact on your information security program.

Regulatory Authority

- 20 U.S. Code § 1094(c)(1)
  - Notwithstanding any other provisions of this subchapter, the Secretary shall prescribe such regulations as may be necessary to provide for:

* **

(B) in matters not governed by specific program provisions, the establishment of reasonable standards of financial responsibility and appropriate institutional capability for the administration by an eligible institution of a program of student financial aid under this subchapter, including any matter the Secretary deems necessary to the sound administration of the financial aid programs, such as the pertinent actions of any owner, shareholder, or person exercising control over an eligible institution;

Regulatory Authority

- 20 U.S. Code § 1094(c)
  - Notwithstanding any other provisions of this subchapter, the Secretary shall prescribe such regulations as may be necessary to provide for:

* * *

(F) the limitation, suspension, or termination of the participation in any program under this subchapter of an eligible institution, or the imposition of a civil penalty under paragraph (3)(B) whenever the Secretary has determined, after reasonable notice and opportunity for hearing, that such institution has violated or failed to carry out any provision of this subchapter, any regulation prescribed under this subchapter, or any applicable special arrangement, agreement, or limitation

Regulatory Authority

- What data is included in the Free Application For Student Aid (FAFSA)?
  - Name
  - DOB
  - SSN
  - Address
  - Email address
  - Phone number
  - Income tax information
- For students AND parents (if needed)

Relevant Department of ED Communications

- "Dear Colleague Letter" GEN-15-18, issued July 29, 2015:
  - https://ifap.ed.gov/dpcletters/GEN1518.html
    - Pertinent sections:
      - reminds institutions of higher education and their third-party servicers of their continuing obligations to protect data used in all aspects of the administration of the Title IV Federal student financial aid programs.
      - The Student Aid Internet Gateway (SAIG) Enrollment Agreement entered into by each Title IV participating institution includes a provision that the institution "[m]ust ensure that all Federal Student Aid applicant information is protected from access by or disclosure to unauthorized personnel." Institutions are reminded that under various Federal and state laws and other authorities, including the HEA; the Family Educational Rights and Privacy Act (FERPA); the Privacy Act of 1974, as amended; the Gramm-Leach-Bliley Act; state data breach and privacy laws; and potentially other laws, they may be responsible for losses, fines and penalties (including criminal penalties) caused by data breaches.

Relevant Department of ED Communications

- "Dear Colleague Letter" issued July 29, 2015:
  - Pertinent sections (cont'd):
    - In addition to other provisions within the SAIG Agreement, *FSA requires institutions to comply with the Gramm-Leach-Bliley Act*. Under Title V of the Gramm-Leach-Bliley Act, financial services organizations, including institutions of higher education, are required to ensure the security and confidentiality of customer records and information. This requirement was recently added to the Program Participation Agreement and is reflected in the Federal Student Aid Handbook.
    - institutions frequently enter into contractual arrangements with other organizations to fulfill institutional obligations with respect to the Title IV federal student financial assistance programs. If your institution has entered into such an arrangement, we remind you of 34 CFR §668.25, which includes a provision that the institution remains liable for any action by its third-party servicers.

Relevant Department of ED Communications

- "Dear Colleague Letter" GEN 16-12, issued July 1, 2016:
  - https://ifap.ed.gov/dpcletters/GEN1612.html
    - Pertinent sections:
      - reminds institutions of their legal obligations to protect student information used in the administration of the Title IV Federal student financial aid programs, as well as the methods the Department will use to assess institutions' capabilities in securing that information.
      - informing institutions that the Department is beginning the process of incorporating the GLBA security controls into the Annual Audit Guide in order to assess and confirm institutions' compliance with the GLBA. The Department will require the examination of evidence of GLBA compliance as part of institutions' annual student aid compliance audit.

Relevant Department of ED Communications

- "Dear Colleague Letter" issued July 1, 2016:
  - Pertinent sections, cont'd:
    - strongly encourages institutions to review and understand the standards defined in the NIST SP 800-171, the recognized information security publication for protecting "Controlled Unclassified Information (CUI)," a subset of Federal data that includes unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Federal policies.

NIST SP 800-171 Requirements

- Limit information system access to authorized users (Access Control Requirements);
- Ensure that system users are properly trained (Awareness and Training Requirements);
- Create information system audit records (Audit and Accountability Requirements);
- Establish baseline configurations and inventories of systems (Configuration Management Requirements);
- Identify and authenticate users appropriately (Identification and Authentication Requirements);
- Establish incident-handling capability (Incident Response Requirements);
- Perform appropriate maintenance on information systems (Maintenance Requirements);

NIST SP 800-171 Requirements

- Protect media, both paper and digital, containing sensitive information (Media Protection Requirements);
- Screen individuals prior to authorizing access (Personnel Security Requirements);
- Limit physical access to systems (Physical Protection Requirements);
- Conduct risk assessments (Risk Assessment Requirements);
- Assess security controls periodically and implement action plans (Security Assessment Requirements);
- Monitor, control, and protect organizational communications (System and Communications Protection Requirements); and
- Identify, report, and correct information flaws in a timely manner (System and Information Integrity Requirement).

Reporting Requirements

- Per "Dear Colleague Letter" issued July 29, 2015:
  - in the event of an unauthorized disclosure or an actual ***or suspected breach*** of applicant information or other sensitive information (such as PII) the institution must ***immediately*** notify FSA at CPSSAIG@ed.gov.
- Jointly notify ED OIG and the Department by calling the ED Security Operations Center (ED SOC) at 202-245-6550. ED OIG will return your call within 24 hours.

Reporting Requirements - LE

- Because schools are required to report these events to the Dept, and ED OIG is the law enforcement agency designated Congress to investigate these matters, then -
- ED OIG is the appropriate law enforcement agency to which events pertaining to the cyber-security of Title IV financial aid programs, related IT systems, and data should be reported.
- Existing protocols will ensure ED OIG is notified if the school reports the matter to the ED SOC.
- Schools may report the incident directly to other LE agencies if they wish, but are not relieved of the requirement to report it to the Dept (and by extension, ED OIG).

Suggestions For Reducing Your Exposure

- Communicate with your Financial Aid Director about relevant Department of ED communications
- Implement NIST SP 800-171 and GLBA Requirements
- Implement a Data Loss Prevention program.
- Scrub legacy systems and isolated network segments for old grade books, class rosters, and professor's class records with student identifiers.
- If in doubt regarding whether an event is reportable, report it.
- The absence of a negative does not make a positive and *vice versa*. The lack of definite proof that a verified intruder took data from your network DOES NOT mean that they did not do it. This would be a *suspected* breach or cyber event and therefore would be reportable.

Suggestions For Reducing Your Exposure

- Work with the Financial Aid Office and the Registrar's office to only maintain data of current students in production systems. Remember that the school receives FAFSA data if a student merely indicates interest. If they do not enroll, there is no business need to keep their data. Archive the data of former or non-current students in a secure offline storage location. If you have the misfortune to be victimized by a data breach, don't let the bad guys get away with the personal data of someone who never attended your school.

Suggestions For Reducing Your Exposure

- Review guides that assist with ensuring compliance with GLBA and that have been incorporated by Federal agencies with oversight on financial institutions in other sectors:
  - https://www.fca.gov/exam/info_tech.html

Final Thoughts

- Please do not let the news media do your reporting for you. This will only bring increased regulatory scrutiny on you, and make the criminal investigation into identifying and prosecuting the responsible parties difficult by delaying our response time.
- If you choose to notify another law enforcement agency first, it does not relieve you of the requirement to notify the Department and ED OIG promptly when a cyber event involving ED records is detected.
- The requirements we have discussed today are already in effect. Please take active steps to start implementing them.

Thank You!

- Questions?
- 1-800-MISUSED - ED OIG hotline
- 202-245-6550 - ED SOC 24x7 number
- www.ed.gov/oig