PROTECTING FINANCIAL DATA FROM DATA BREACHES

Up to a 100,000 taxpayers could have been compromised due to hackers who posed as students and completed the FAFSA form by using the Internal Revenue Service (IRS) Data Retrieval Tool (DRT), according to an article in the April 6, 2017 *The New York Times*.[1] The DRT is used to automatically populate student and parent tax information on the Free Application for Federal Student Aid (FAFSA). The IRS was forced to send out almost 100,000 letters alerting taxpayers of the risk to their data. The agency believes that almost 8,000 fraudulent returns were filed and refunded for a total of $30 million.

According to an April 27, 2018 article in *The Washington Times*, on December 11, 2017,[2] Jordan Hamlett plead guilty to false representation of a Social Security number after investigators caught him repeatedly using President Trump's Social Security number, date of birth, and other information to complete the FAFSA and attempt to retrieve Mr. Trump's tax returns through the IRS. He was sentenced to 18 months in federal prison.

Federal Student Aid (FSA) was forced to take down the IRS DRT tool for much of the 2017-2018 award year and was not able to implement a solution that allowed it to reinstate the IRS DRT tool until the beginning of the 2018-2019 FAFSA cycle.[3] The solution encrypts the taxpayer's information and hides it from the applicant's view on both the IRS DRT web page and on the FAFSA web pages. However, the information sent to educational institutions via the Institutional Student Information Records (ISIRs) document includes all of the tax information that was transferred into the FAFSA using the IRS DRT. If any corrections need to be made to the ISIR, they must be made by the institution.

On October 16, 2017, the Department of Education advised institutions of a new threat, where criminals are seeking to extort money from school districts and other education institutions on the threat of releasing sensitive data from student records.[4] According to the October 16, 2017 electronic announcement, there are threats of violence, shaming, or bullying children unless payment is received. FSA warned that attackers are likely targeting school districts with weak data security, or well-known vulnerabilities that allow the attackers to gain access to sensitive data. "This may be in the form of electronic attacks against school district computers or applications, malicious software, or even through phishing attacks against staff or employees." The electronic announcement stated that while these new threats have been directed only to K12, institutions of higher education are warned that they are required to notify FSA of any data breaches pursuant to the Gramm-Leach-Bliley Act (GLBA), their Title IV participation, and their SAIG agreements. ED encouraged educational institutions to conduct security audits, ensure proper audit logs are created, train staff and students on data security best practices, and review all sensitive data to limit access from the outside.

More recently, FSA issued an electronic announcement on August 31, 2018, stating that it had identified a malicious phishing campaign that may lead to potential fraud associated with student

1 See: https://www.nytimes.com/2017/04/06/us/politics/internal-revenue-service-breach-taxpayer-data.html.
2 See: https://www.washingtontimes.com/news/2018/apr/27/attempts-retrieve-donald-trumps-tax-returns-yields/.
3 See: https://ifap.ed.gov/eannouncements/050317StatusoftheFAFSAIRSDataRetrievalTool.html.
4 See: https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html, pg. 1.

refunds and aid distributions.[5] Attackers are using a phishing email to obtain access to student accounts at multiple institutions of higher education. The Department concluded that the attackers have done some level of research and understand the schools' use of student portals and methods.

On July 29, 2015 in Dear Colleague letter GEN-15-18[6] and again on July 1, 2016 in Dear Colleague letter GEN-16-12[7], the Department of Education reminded institutions of their legal obligations to protect student information used in the administration of Title IV Federal student aid funds. DCL GEN-16-12 warned institutions that the Department is beginning the process of incorporating the Gramm-Leach-Bliley (GLBA) security controls into the Annual Audit Guide in order to assess and confirm institutions' compliance with the GLBA.

The sources of Title IV legal obligations to ensure the security and confidentiality of customer records include:

- Program Participation Agreement (PPA);
- Gramm-Leach-Bliley Act (GLBA), P.L. 106-102;
- Student Aid Internet Gateway (SAIG) Enrollment Agreement; and
- Family Educational Rights and Privacy Act (FERPA).

All institutions must sign a Program Participation Agreement (PPA) in order to participate in the Title IV programs. The General Terms and Conditions included in the PPA require institutions to agree to comply with the Standards for Safeguarding Customer Information, 34 C.F.R. § 314, issued by the Federal Trade Commission (FTC), as required by the GLBA, since institutions that are eligible to participate in the Title IV programs are considered financial institutions per the GLBA because they are engaged in providing financial products, such as student loans. These Standards are intended to ensure the security and confidentiality of customer records and information, and any breach to the security of student records is considered a "potential lack of administrative capability." The elements of the Safeguards Rule[8] include:

- Designating an employee(s) to coordinate the information security program;
- Identifying 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 that are in place. At a minimum, risk assessment should include:
    - Training employees and management;
    - Reviewing information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and
    - Detecting, preventing and responding to attacks, intrusions, or other systems failure.

5 See: https://ifap.ed.gov/eannouncements/083118ActivePhishingCampaignTargetStudentEmailAccount.html.
6 See: https://ifap.ed.gov/dpcletters/GEN1518.html.
7 See: https://ifap.ed.gov/dpcletters/GEN1612.html, pg. 2.
8 See: 34 C.F.R. § 314.4.

- Designing and implementing information safeguards to mitigate the risks identified in the required risk assessment, and regularly test and monitor the effectiveness of those safeguards;
- Overseeing service providers by taking reasonable steps to select and retain service providers that are capable of implementing and maintaining appropriate safeguards for the customer information at issue and require service providers, by contract, to implement and maintain such safeguards; and
- Evaluating and adjusting the information security program in light of changed circumstances.

Under the Student Aid Internet Gateway (SAIG) Enrollment Agreement[9], entered into by each Title IV participating institution, an institution "must ensure that all users are aware of and comply with all of the requirements to protect and secure data from Departmental sources using SAIG."

The HEA also requires institutions to maintain appropriate institutional capability for the sound administration of the Title IV programs, which includes compliance with the Family Educational Rights and Privacy Act (FERPA), which generally prohibits institutions from having policies or practices that permit the disclosure of education records or personally identifiable information (PII) contained in the education records without the written consent of the student, unless an exception applies. Any data breach resulting from a failure of an institution to maintain appropriate and reasonable security policies and safeguards could also constitute a FERPA violation.[10]

Data breaches continue to reoccur. The Department has made it clear that institutions must comply with cybersecurity regulations. To ensure that institutions are able to comply, it offers a cybersecurity compliance website,[11] which includes the rules, the relevant guidance, cybersecurity frequently asked questions, and the procedures for reporting a suspected or known breach on the date of detection.

- While there have been no changes as yet to the Audit Guide, the Department said in an FSA Conference presentation in 2017 that the Department was drafting audit language to be used by auditors to determine whether institutions were meeting the requirements of the GLBA. The draft language provided by ED would require auditors to make the following determination:
    - Institution has designated an individual to coordinate information security program;
    - Institution has performed the risk assessment; and
    - Institution has aligned each safeguard with each risk identified in the risk assessment.
- The Department has the authority to fine institutions that do not comply with the requirement to self-report data breaches – up to $54,789 per violation per 34 C.F.R. § 36.2; and

9 See: https://ifap.ed.gov/dpcletters/attachments/20152016SAIGFormWatermarked.pdf, pg. 31.
10 See: https://ifap.ed.gov/dpcletters/GEN1518.html, pg. 2.
11 See: https://ifap.ed.gov/eannouncements/Cyber.html.

- Institutions are obligated to implement security policies that protect students' PII.

As pointed out in the January 12, 2018 Updated Cybersecurity Compliance Frequently Asked Questions[12], institutions should worry about data security because the educational sector has an initial level of security maturity, which results in high risk and because the educational sector is a "rich trove of email addresses and credentials, financial information, research, and development."

Sharon H. Bob, Ph.D. is a Higher Education Specialist in the Powers Pyles Sutter & Verville Education practice. She advises educational institutions regarding issues related to their participation is the federal student assistance programs, accreditation, licensure, education tax credits, and related regulatory matters. Sharon can be reached at Sharon.Bob@PowersLaw.com or 202-872-6724.

12 See: https://ifap.ed.gov/eannouncements/011218UpdatedCyberComplianceFAQ.html, pg. 1 of FAQ.