THE LACK OF RESPONSIBILITY OF HIGHER EDUCATION INSTITUTIONS IN ADDRESSING PHISHING EMAILS AND DATA BREACHES

MUXUAN (MURIEL) WANG†

ABSTRACT
Higher education institutions (HEIs) are highly susceptible to cyberattacks, particularly those facilitated through phishing, due to the substantial volume of confidential student and staff data and valuable research information they hold. Despite federal legislations focusing on bolstering cybersecurity for critical institutions handling medical and financial data, HEIs have not received similar attention. This Note examines the minimal obligations imposed on HEIs by existing federal and state statutes concerning data breaches, the absence of requirements for HEIs to educate employees and students about phishing attacks, and potential strategies to improve student protection against data breaches.

INTRODUCTION
On September 13, 2022, members of Duke University received fraudulent (or “phishing”) messages with an “urgent warning” related to their Duke account or an offer of false job opportunities.1 Many alarmed recipients followed the link provided in the deceptive emails and unwittingly input their passwords and Multi-Factor Authentication (MFA) codes, allowing hackers to compromise their accounts.2 Subsequently, the compromised accounts were used to send further fraudulent messages from Duke email addresses, reaching thousands of Duke members.3 Fortunately, with the help of the “report phish” button installed in the Duke

† Duke University School of Law, J.D. and LL.M. in International and Comparative Law expected May 2024; Scripps College, B.A., May 2017.
email system in October 2019, the Information Technology Security Office timely identified and blocked the compromised accounts and stopped the spread of phishing emails. 4 Nevertheless, the fact that thousands of suspicious emails were sent around campus through the compromised Duke email accounts highlights the imminent danger of data breaches in higher education institutions. 5 In similar instances, when institutions have failed to promptly halt the propagation of phishing emails, direct damages to the school can be as high as $50 million.6

Higher education institutions (“HEIs”) are highly vulnerable to data breaches, especially those achieved by phishing.7 On one hand, HEIs are hubs of large-volume confidential student & staff data and sensitive cutting-edge research data with potential economic value, which makes them favorable targets for cyber-attacks.8 On the other hand, students who actively use university networks are typically not well-informed about countering significant cybersecurity risks, making them susceptible targets for phishing attempts. 9 The U.S. Department of Education also acknowledges this two-fold vulnerability and notes that “computer systems at colleges...hold many of the same records as banks but are much

5 The National Institute of Standards and Technology defines data breach as “an incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.” See Glossary, SMALL BUSINESS CYBERSECURITY CORNER (last visited Dec. 2, 2022), https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary.
6 Jo Rushton, 50+ Phishing Statistics You Need to Know – Where, Who & What is Targeted, TECHOPEDIA.COM (last updated Mar.1, 2024) (noting that “the phishing attack caused the UVM system to go down for 28 days, and employees were forced to clear 1,300 servers of malware”), https://www.techopedia.com/phishing-statistics.
9 See e.g., Roderic Broadhurst, et al., Phishing and Cybercrime Risks in a University Student Community, 2 (1) INT’L J. OF CYBERSECURITY INTEL. & CYBERCRIME, 4 (2019) (study showing that international students and first year students in college are deceived by significantly more scams than others); Phishing Scams Often Target Stanford Students, STANFORD UNIV. IT (Oct. 13, 2023), https://uit.stanford.edu/news/phishing-scams-often-target-stanford-students (noting that students are especially vulnerable to phishing).
This vulnerability is further evidenced by the frequency of breaches within the education sector. Between 2005 and 2021, the sector endured 1,850 data breaches, affecting over 28.6 million records. Notably, among these records, approximately 87% came from universities.

There is minimal regulation in place to protect students from data breaches. Presently, there are statutes obliging financial and medical institutions to establish internal cybersecurity measures to ensure the confidentiality and integrity of their data. This includes enhancing IT infrastructure’s resilience to cyberattacks and offering specific education for their employees. In addition, many firms in unregulated industries proactively implement internal education programs to raise awareness against fraud. Nevertheless, while the implementation of robust cybersecurity measures is commonplace in financial and medical industries, higher education lags behind. Despite the substantial risk of data breaches faced by HEIs, the responsibilities and liabilities they bear remain unclear. This paper analyzes three key questions: first, what are the general duties current regulations impose on HEIs regarding data breaches; second, whether HEIs have a responsibility to educate their employees and students regarding phishing attacks; and third, what are some ways for HEIs to enhance the protection of students against data breaches.

Part I analyzes the limited mechanisms to impose liability on HEIs for general data breaches. It starts with an overview of existing federal and state statutes that might impose specific responsibilities on HEIs. The analysis then shifts to the lack of private right of action in HEIs’ data breaches. Finally, this section reviews how a combination of private

---


12 Id.


14 Id.

lawsuits under tort law and reputational harm might give HEIs some incentive to build a more secure computer system.

Part II focuses more narrowly on phishing and examines the circumstances under which HEIs must provide adequate training for their employees on cybersecurity issues. Contrarily, HEIs do not have any obligation to educate their students about data security.

Part III evaluates several methods to enhance the protection of students against data breaches. Many congressional acts were proposed to raise the liability of HEIs to incentivize them to reduce the incidents of data breaches. In addition, several executive orders and guidelines from federal agencies were issued to help HEIs understand the best steps to reduce further harm to victims. Further, after data breaches occurred, many HEIs also started to provide remedial programs.

I. HEIS HAVE LIMITED LIABILITY FOR DATA BREACHES

Currently, no state or federal laws and regulations mandate specific requirements for all HEIs to defend against data breaches. Furthermore, victims lack federal private right of actions against HEIs in cases of data breaches. Nevertheless, class action lawsuits emerging from state law and huge financial cost of data breaches may serve as incentives for HEIs to enhance their data security.

A. Existing state and federal laws do not impose a specific requirement on HEIs to defend against data breaches.

While many regulations at the federal and state level impose obligations to HEIs to take security measures to enhance data security, most of those obligations are either weakly stated or are peripheral to the prevention of data breaches.

On the federal side, the most directly applicable regulation is the Family Educational Rights and Privacy Act (FERPA), which covers educational institutions that receive funds from programs administered by the U.S. Department of Education, including “postsecondary institutions, such as colleges and universities.” FERPA generally regulates the release of education records but provides no clear explanation of HEIs’ obligation regarding data breaches. Instead, the two primary focuses of FERPA grant students (or parents) the right to access their educational records and

17 To which educational agencies or institutions does FERPA apply?, PROTECTING STUDENT PRIVACY (last visited Dec. 2, 2022), https://studentprivacy.ed.gov/faq/which-educational-agencies-or-institutions-does-ferpa-apply.
18 20 U.S.C. § 1232g.
prevent HEIs from actively disclosing educational records to third parties without adequate consent. The Department of Education also explicitly states that FERPA “does not require educational institutions to adopt specific security controls.” Therefore, in the context of data breaches, FERPA serves, at best, as an affirmation that data protection is essential and beneficial.

In addition to FERPA, a few federal regulations originally designed for non-education sectors can impact HEIs under specific circumstances. Generally, institutions may face penalties for the negligent disclosure of personal information under acts such as the Health Insurance Portability and Accountability Act (HIPAA), the Computer Fraud and Abuse Act (CFAA), the Gramm-Leach-Bliley Act (GLBA), and the Federal Trade Commission (FTC)’s Red Flags Rule. While some HEIs may fall under the regulatory scope of these acts, their application is not widespread across all HEIs.

An HEI that operates a medical hospital and submits claims for reimbursement of medical expenses to third parties is generally subject to HIPAA. For the enforcement of GLBA, the FTC considers HEIs to be financial institutions when they “appear to be significantly engaged in lending funds to consumers.” HEIs can also fall within the jurisdiction of the Red Flags Rule as “creditors.” Compared to FERPA, these laws and regulations impose more specific responsibilities on regulated HEIs. For instance, regulated HEIs must maintain “reasonable and appropriate administrative, technical and physical safeguards,” identify “reasonably

foreseeable internal and external risks,” 26 and implement a written “identity theft prevention program.” 27

However, given that HEIs are not the primary entities targeted by these acts, federal agencies overseeing them naturally place more emphasis on other institutions. For example, among the twenty closed GLBA cases stored in the FTC legal library, only one concerned a university. 28 Furthermore, as illustrated below, because these regulations do not grant a private right of action, HEI’s compliance with these requirements often remains unchecked.

Regarding state legislation, all fifty states have data breach notification laws that require the affected party to notify the government or consumers in the event of a data breach involving personal information such as “names coupled with social security numbers, birth dates, [and] financial information.” 29 Nevertheless, only a few states have enacted statutes that explicitly require the regulated entities to actively enhance their data security measures. 30 Even within these states, statutes typically employ the vague standards of “reasonableness” or “industry practice” and do not provide specific guidelines for regulated entities to follow. 31 Consequently, in most states, HEIs are obligated only to retroactively report a data breach and are not required to take specific proactive measures to defend themselves from future potential breaches.

---

26 16 C.F.R. § 314.4.
28 Legal Library: Cases and Proceedings, “Gramm Leach Bliley Act,” FEDERAL TRADE COMMISSION (last visited Jan. 6, 2023). https://www.ftc.gov/legal-library/browse/cases-proceedings?sort_by=search_api_relevance&items_per_page=20&search=gramm+leach+bliley+act&field_competition_topics=All&field_consumer_protection_topics=All&field_federal_court=All&field_industry=All&field_case_status=All&field_enforcement_type=All&search_matter_number=&search_civil_action_number=&start_date=&end_date=.
30 See William McGeveran, The Duty of Data Security, 103 MINN. L. REV. 1135, 1154 (note 90) (2019) (noting that states including MA, NY, CA, OH, CT, MD, NV, OR, TX have limited statutes regarding duty of data security); Michelle J. Anderson, Jim Halpert, New Student Data Privacy Laws: Top Points for School Contractors And K-12 Education Sites, Apps And Online Service, 20 NO. 1 CYBERSPACE LAW, 6 (2015) (noting that several states have enacted regulations imposing obligation to vendor’s for the data security of student data).
31 See McGeveran, supra 28 at 1158.
B. No private rights of action for data breaches under federal regulations

A central insufficiency in current federal regulatory schemes is the lack of a private right of action. In other words, there is no mechanism for individuals to sue institutions when their personal data is breached.

First, most jurisdictions hold that FERPA does not create a private right of action. 32 The Supreme Court has ruled that “[FERPA’s] nondisclosure provisions fail to confer enforceable rights,” 33 a stance subsequently interpreted by many circuits to mean that FERPA does not “create legal rights, the invasion of which creates standing.” 34 For example, in a 2020 case involving a data breach in an education agency, the Northern District of Illinois determined that an alleged violation of FERPA did not confer Article III standing arising from the data breach of an educational testing platform.35

Similarly, courts have consistently held that neither GLBA nor HIPAA creates a private right of action for individuals to bring lawsuits against alleged violations.36 GLBA and HIPAA are generally enforced by the FTC and the Department of Health and Human Services (HHS), respectively. With limited capacity in both investigation and enforcement, federal agencies tend to “favor voluntary compliance over penalties and sanctions,” leaving victims without personal remedies. 37 As a result, although GLBA and HIPAA impose the most detailed and rigid requirements regarding data breach and data security, they still do not serve as a strong enough incentive for HEIs to implement the best cybersecurity solutions.

34 Gaylor v. Mnuchin, 919 F.3d 420, 426 (7th Cir. 2019) (quoting Sterk v. Redbox Automated Retail, LLC, 770 F.3d 618, 623 (7th Cir. 2014)). See also Kyles v. J.K. Guardian See. Servs., Inc, 222 F.3d 289, 294 (7th Cir. 2000) (explaining that statutory standing “depends in great measure on the particular rights conferred”).
Unlike the narrow application of FERPA, a few states have recognized that a violation of HIPAA or GLBA can serve as evidence in establishing a standard of care in tort claims, forming the basis of breach of contract, or proving other violations of state statutes. Nevertheless, it is important to note that the violation of HIPAA and GLBA themselves do not create a private right of action. Their use as supplementary evidence in state law claims is still limited and peripheral: only some HEIs fall under the purview of these statutes, and the dearth of enforcement complicates demonstrating noncompliance with such regulations.

C. Class actions brought by victims against HEIs might serve as an incentive

Despite the lack of private right of action in federal statutes, individuals impacted by university data breaches have sought remedies through litigation, frequently as part of class actions, relying on traditional tort and contract theories. Since these theories are not tailored towards cybersecurity and data breaches, the outcome of these lawsuits is uncertain. Nevertheless, perhaps driven by concerns about reputational harm, HEIs are often willing to settle lawsuits with promises to strengthen their cybersecurity programs to prevent future data breaches.

In February 2016, a former student of the University of Central Florida initiated a class-action lawsuit against the university, alleging negligence shortly after the school acknowledged a hacking incident that exposed 63,000 Social Security numbers. Approximately two years later, the university settled the case, agreeing to pay $500 in damages to each of

---

38 See Acosta v. Byrum, 638 S.E.2d 246, 251 (N.C. Ct. App. 2006) (holding that HIPPA can be used to “establish the standard of care”).
39 See Dinerstein v. Google, LLC, 484 F.Supp.3d 561, 584 (N.D. Ill. 2020) (noting that “a contract claim incorporating HIPAA is such a ‘more stringent’ measure and is thus not preempted by the federal statute”).
41 See supra pages 4–6.
the five named plaintiffs and covering attorney fees. Importantly, as part of the settlement, the university committed to initiatives such as “purchasing new forensic software, implementing multi-factor authentication for employees and increasing awareness about how to best protect personal information.” Additionally, the university pledged to allocate an “additional $1 million annually to protect students’ and employees’ personal information.”

In 2019, victims of a hacking incident involving the student and employee portal filed a class-action lawsuit accusing Wichita State University of “negligence, breach of implied contract, becoming unlawfully enriched, and violating Kansas consumer protection law.” The university settled the lawsuit in 2020, agreeing to provide payments of up to $300 per person to those with out-of-pocket expenses related to the data breach incident.

Washington State University experienced a data breach resulting from a stolen hard drive in April 2017. The hard drive allegedly contained names, Social Security numbers, and educational and personal health information for 1 million individuals. The case was settled with a substantial payment, amounting to $3.2 million, enabling affected individuals to be reimbursed up to $5,000 each for documented out-of-pocket expenses related to the data breach incident.

---

44 Id.
49 Id.
pocket costs. The university subsequently agreed to update its policies and procedures and enhance cybersecurity by storing backup data in a more secure location, conducting data security assessments and audits, and providing additional training to staff.

Nevertheless, not all victims of data breaches choose to bring class action lawsuits against HEIs, and even when they do, not all lawsuits culminate in satisfying settlements. Most lawsuits arising from data breaches face the significant challenge of “proving injury” to qualify for Article III standing in court, especially when there is no proof that the breached information has caused actual monetary damage to the plaintiffs. Consequently, utilizing class actions can only be the last resort for victims who otherwise struggle to obtain relief under federal or state statutes.

D. Financial loss cannot be a strong-enough incentive

The financial losses incurred due to a data breach are considerable. According to the Ponemon Institute’s “2017 Cost of Data Breach Study,” the cost per record for data breaches in educational institutions in the U.S. is $245, which is $20 more than the average cost per record for all data breaches. Given that university data breaches may affect tens of thousands of records, the overall cost to HEIs can quickly escalate to

50 WSU Security Incident Class Action Settlement, TOP CLASS ACTIONS (May 22, 2019); see also www.WSUSettlement.com.
millions of dollars. This financial impact may be significant enough to draw HEIs’ attention to the gravity of data breaches.

For example, in 2013, a data breach at Maricopa County Colleges exposed the social security numbers and banking information of over 2 million people, resulting in a staggering cost of over $26 million for the school to address the losses. In addition to expenses for legal matters, credit monitoring, call center operations, and public relations, the university had to allocate $7.5 million for post-data breach consulting and computer system repair to enhance the security of its IT systems.

Nevertheless, it may be unrealistic to expect HEIs to invest significantly in more robust protections for student data solely due to the potential costs of data breaches. The perceived likelihood of experiencing a data breach might not be high enough to justify allocating extensive budgets to the issue. After all, many HEIs may opt for the alternative approach of purchasing cybersecurity insurance to cover the potential costs.

II. HEIS ARE LESS OBLIGED TO EDUCATION AGAINST PHISHING ATTEMPTS

HEIs are less accountable for data breaches caused by fraudulent phishing emails (where employees or students accidentally gave out their confidential information) than those caused by hackers breaking through the information system purely through technological means. There are fewer mechanisms mandating HEIs to provide adequate training to their employees. Regarding students, the analysis below indicates that the university’s responsibility only extends to personal safety and does not encompass cybersecurity education.

55 See Matt Zalaznick, Top 10 States for Data Breaches Warn of Constant Cyber Threat to Higher Ed, UNIVERSITY BUSINESS (Apr. 11, 2023), https://universitybusiness.com/top-10-states-college-university-data-breaches-higher-ed-cybersecurity/ (noting that “nearly 2,700 education cyberattacks have compromised 32 million education records over the last two decades”, which amounts to 11,851 records per cyberattack).
56 Id. at 253.
57 Id.
58 Research over 447 colleges reveal that over half of these institutions carry cyber insurance with average coverage of $7.8 million, although only 6.9% have experienced a serious data breach. See Rick Seltzer, As Cybersecurity Threat Rages, Colleges Invest in Risk Prevention and Pay Higher Insurance Premiums, HIGHER ED DRIVE (Oct. 6, 2022), https://www.highereddrive.com/news/as-cybersecurity-threat-rages-colleges-invest-in-risk-prevention-and-pay-h/633548/.
Obligations for HEIs to train employees arises from the GLBA and HIPPA. Although these acts are primarily designed for financial and health industries, they may apply to HEIs under specific circumstances. For instance, HEIs that frequently lend out loans through student aid are regulated by the GLBA and the “Safeguards Rule” issued by the FTC.

As noted above, FTC appears to primarily focus on the more traditionally defined financial institutions and may not strictly enforce its rules over HEIs. Nevertheless, the Safeguards Rule does impose a requirement for staff training programs on qualifying HEIs. Section 314.3(a) of the Safeguards Rule obliges the institutions to develop a comprehensive written information security program. Section 314.4(e) then specifies that one of the nine elements of such a program is “policies and procedures to ensure that personnel are able to enact your information security program.” One of these procedures includes “providing your personnel with security awareness training that is updated as necessary [to counter reasonably foreseeable risks].” The FTC emphasizes that businesses should “insist on specialized training for employees . . . and verify that they’re keeping their ear to the ground for the latest word on emerging threats and countermeasures.” Therefore, despite the potential lax enforcement, the Safeguards Rule serves as a mechanism to encourage HEIs to adopt training programs that help prevent phishing threats emerging from careless employees.

Similarly, the Security Rule under HIPAA requires institutions to adopt “security standards that take into account the need for training persons who have access to health information.” This, like the Safeguards Rule, places a responsibility for cybersecurity training on employees of applicable HEIs. Nevertheless, as mentioned earlier, the core shortcoming of federal statutes lies in their dependence on federal agencies, which might lack the capacity and willingness to enforce these statutes fully. Therefore, even though these mechanisms exist, they are unlikely to be fully effective.

When it comes to data breaches caused by students, the university bears even less responsibility. Unlike their obligation to prevent criminal

---

59 See supra note 20 and 21.
61 See supra page 6.
62 16 C.F.R. § 314.3(a).
63 16 C.F.R. § 314.4(e)(1).
64 Id.
acts such as sexual harassment, current regulations do not hold HEIs responsible for educating students and raising awareness of phishing emails and cyber-attacks.67

HEIs are typically held responsible for failure to educate students on areas where they possess specialized responsibilities. The Restatement (Second) of Torts specifies that “there is no duty…to control the conduct of a third person as to prevent him from causing physical harm…unless a special relation…imposes a duty upon the actor to control the third person's conduct, or…gives to the other a right to protection.”68 Generally, HEIs are viewed as having a duty to control students’ conduct and “to protect or warn their students from foreseeable violence in the classroom or during curricular activities.”69 Courts are usually willing to establish a breach of duty when the precautions taken by the university to prevent harassment and assault are proven inadequate.70 Some specialized responsibilities are created by specific legislations. For example, Title IX and the Clery Act impose the special responsibility on HEIs to prevent sexual harassments in order to protect equal access to.71 Consequently, over 600 HEIs have adopted online sexual assault prevention courses as part of compliance with Title IX.72

In contrast to harassment and assaults leading to physical injury or sexual assaults, phishing attacks do not fall under any special responsibility of HEIs. In the absence of physical harm, even when students’ accounts are compromised by phishing emails, HEIs do not seem to breach any of their duties. As a result, HEIs lack the incentive to establish comprehensive cybersecurity education programs and enforce student compliance in these programs to prevent data breaches.

---

67 Title IX requires schools that receive federal funding to take steps to prevent sexual harassment of students. See Child Abuse and Sexual Harassment, 1 EDUCATION LAW: FIRST AMENDMENT, DUE PROCESS AND DISCRIMINATION LITIGATION § 4:12
68 RESTATEMENT (SECOND) OF TORTS, § 315 (1965).
69 Regents of Univ. of California v. Superior Ct., 4 Cal. 5th 607, 619, 413 P.3d 656, 663 (2018).
70 See, e.g., Escue v. N. Okla, Coll., 450 F.3d 1146, 1156, (10th Cir. 2006) (applying Oklahoma law); see also Takla v. Regents of the Univ. of Cal., 2015 WL 6755190 at *5 (C.D. Cal. 2015) (applying California law).
72 Id.
III. POTENTIAL METHODS TO PROTECT STUDENTS FROM PHISHING AND CYBER-ATTACKS IN THE FUTURE

Two crucial steps should be taken to bolster the protection of student and employee data at HEIs. First, incentives should be established to encourage HEIs to prioritize and address data security concerns. Second, HEIs should acquire necessary data security knowledge and adopt the most effective and efficient measures for preventing data breaches and minimizing harm.

A. Government should incentivize HEIs to install methods to prevent data breach

Incentives for HEIs to allocate more time and resources toward preventing data breaches can be driven by two directions: negative incentives involving penalties for failure to protect, and positive incentives where HEIs receive benefit and support for implementing necessary measures.

Negative incentives materialize through legislation that heightens liability for HEIs. Several bills introduced in Congress seek to place additional responsibilities on HEIs based on existing regulations. An illustrative case is the Student Privacy Protection Act, introduced to the Senate in July 2015. The act aimed to broaden FERPA’s coverage, mandating HEIs “to establish information security practices to protect students’ education records and personally identifiable information” and “to notify parents of breaches or security violations.” Another significant bill was the American Data Privacy and Protection Act introduced to the House in June 2022. This legislation included provisions aimed at imposing data security obligations on a wide array of entities, including HEIs. While these bills have not been passed into federal law, they signify an intention to extend the stricter requirements currently applicable only under specific legislations like GLBA, HIPAA, and state laws to all HEIs. Faced with potential federal requirements, HEIs may experience pressure to implement changes.

Another negative incentive stems from the private right of action. As introduced earlier, no federal data privacy or security law in the United States explicitly grants victims a private right of action. With no federal law to rely on, some victims resort to bring class actions under traditional

73 S.1341, 114th Congress (2015-2016).
74 S.1341, 114th Congress (2015-2016).
76 Supra pages 7–8.
tort theory, with only a few achieving successes. The creation of a private right of action for violations of data privacy laws, such as FERPA, GLBA, and HIPAA, would provide victims with more avenues to hold HEIs accountable for data breaches. This, in turn, would offer HEIs greater incentive to adopt robust cybersecurity measures, as improved protection of student data could help mitigate potential litigation costs. Notably, some legislations in other countries have already granted a private right of action to victims. For example, Article 82(1) of the General Data Protection Regulation (GDPR) in Europe states that “any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.” This could serve as a potential model for U.S. legislations to consider.

Apart from legislative attempts, judicial activities such as the interpretation of vicarious liability may serve as another negative incentive for HEIs to provide more effective anti-phishing training, particularly to their employees. Employers are vicariously liable for “tortious acts” of their employees. The difficulty here is that unlike regular data breaches incidents where hackers break through the firewall, data breaches caused by phishing emails sent out from an employee’s compromised email account do not directly constitute a breach of duty. Since breach of duty is an essential element of a tort claim, if no breach of duty is involved, there would be no liability to be imputed. Additionally, it is also challenging for plaintiffs to demonstrate that data breaches resulted from insufficient employee training against spear phishing attacks.

Nevertheless, some courts have rendered decisions indicating that employers may be held liable for phishing emails originating from their employees’ compromised accounts. Invoking the “imposter rule,” a district court in 2015 ruled that the party receiving fraudulent wire instructions was “in the best position to prevent the forgery” and should bear responsibility for their own loss. In contrast, in 2018, the Sixth

---

77 Supra pages 8–10.
78 Art. 82 Right to compensation and liability, GEN. DATA PROT. REGUL. (GDPR), (Apr. 14, 2016), https://gdpr-info.eu/art-82-gdpr/.
80 RESTATEMENT (FIRST) OF TORTS § 4 (1934).
Circuit, citing the same rule from the previous case, found a genuine issue of fact on which party should bear more responsibility and called for the “apportion the loss according to their comparative fault.” As illustrated by these two cases, courts have not established a definitive standard for determining liability in email compromise cases. However, the potential for liability may prompt employers, including HEIs, to exercise increased diligence in bolstering their employees’ resilience against phishing attempts.

Positive incentives, whether in the form of financial or technological support from the federal government, can also significantly aid HEIs. For example, a recent bill introduced to the Senate named “Student Right to Know Before You Go Act of 2022” aimed to establish a “new higher education data system” under the Department of Education. The primary goal is to “minimize…the privacy risks to individuals…that could result from data breaches of any system operated by [HEIs].” This legislative initiative seeks to create a secure governmental education data system, thereby alleviating some of the burdens on HEIs in maintaining sensitive student data. If such a system is implemented, HEIs could potentially avoid the necessity of allocating extra budgetary resources while still attaining a heightened level of data security.

B. HEIs should adopt the best practices

HEIs should also implement the optimal methods for preventing future data breaches and safeguarding the data of their students and staff. These measures can be broadly categorized into three aspects: strengthening information systems, providing education to students and staff, and addressing existing data breaches through remedial actions.

Federal agencies have implemented various initiatives to support HEIs in building more robust information systems to fend off cyber-attacks. The Department of Education’s Student Privacy Policy Office provides specific guidance through a dedicated website to assist HEIs in constructing secure information systems. The Federal Student Aid Office maintains an updated information page, highlighting recently identified data security risks in higher education. Additionally, the

---

National Institute of Standards and Technology (NIST) published guidance in February 2020, outlining best practices for protecting Controlled Unclassified Information. These programs contribute to helping HEIs establish a foundational defense against cyber-attacks. For instance, effective filter systems can minimize the volume of phishing emails reaching the inboxes of students and staff. Similarly, multi-factor authentication programs play a crucial role in preventing hackers from accessing confidential information, even in cases where they have obtained account numbers and passwords.

Many HEIs have taken steps to raise awareness of phishing emails and other cyber-attacks, educating students on essential protective measures such as maintaining stronger passwords and practicing password rotation. Institutions like the University of Rochester, Stanford University, and the University of Pittsburgh have established webpages guiding students on identifying and reporting scams. Additionally, various HEIs have organized activities and events, including cybersecurity festivals and campaigns, to further promote cybersecurity awareness.

While no specific data demonstrates the success of these measures, they are likely contributing to enhancing students’ knowledge of the issue. As a study of online sexual harassment prevention programs reveals, digital training programs “can be effective at providing students with a foundation of knowledge and awareness that can be built on by future efforts.” The implementation of mandatory online training on

---

94 Zapp et al., supra note 62, at NP2341.
cybersecurity could potentially serve as an effective tool in equipping students with the necessary knowledge to combat phishing and other cyber-attacks. There is yet to be a mandatory cybersecurity education program for HEIs, probably because of the lack of legislative enforcement. Nevertheless, such a program might be adopted by HEIs in the future, accompanied by more specific legislation.

Finally, in the unfortunate event of a data breach, HEIs must be well-versed in the best strategies to minimize further damage. There are myriad harms that can affect data processors and owners beyond data leakage concerns. For instance, if a person uses the same password for other accounts, the hackers could also compromise those accounts.\(^\text{95}\) Lost confidential data can also be used to compose fraudulent messages or make fraudulent payments. Therefore, notification and assistance to victims are crucial to prevent further harm. For example, UCLA, following a data breach in 2017, notified over 30,000 students of the potential compromise of their personal data and offered one year of identity-protection service.\(^\text{96}\) Similarly, Tidewater Community College, after a March 2016 data breach, provided free credit monitoring services to affected individuals.\(^\text{97}\) In addition to notifications and related services, UC Berkeley enlisted a forensics expert,\(^\text{98}\) the University of Maryland launched a large-scale investigation into the breach,\(^\text{99}\) and both the University of Central Florida and Indiana University set up call centers to address victim inquiries.\(^\text{100}\)

The outlined measures present effective ways for HEIs to bolster their cybersecurity and minimize the impact of data breaches resulting from phishing attacks. It's important to note that not all HEIs that have experienced data breaches implement every mentioned measure. If all HEIs receive more guidance on the best way to treat an existing data breach, they may be able to deal with data breach incidents more effectively.

CONCLUSION

As the general public increasingly prioritizes data security concerns, the prevention of data breaches in HEIs is gradually becoming

\(^{95}\) See e.g., Aranza Trevino, \textit{Why Can’t I Use the Same Password for Everything?}, KEEPER (May 4, 2023), https://www.keepersecurity.com/blog/2023/01/04/can-i-use-the-same-password-for-everything/.

\(^{96}\) Goldstein, \textit{supra} note 47, at 249–50.

\(^{97}\) Id.

\(^{98}\) Id.


\(^{100}\) Id.
a prominent topic. However, this note’s analysis of existing regulations reveals a lack of effective and specialized legislation, both at the federal and state levels, to standardize cybersecurity practices in HEIs. Additionally, there appears to be a dearth of enforcement mechanisms to encourage HEIs to educate their numerous vulnerable employees and students on effective ways to protect themselves against cyber-attacks.

To fortify the protection of student and employee data, it is imperative to enact more legislation that holds HEIs accountable in specific ways and implement well-developed programs to equip them with robust protections for their students and employees. Until such legislation is enacted, despite remediation efforts, student data is likely to remain highly vulnerable to cyberattacks.
APPENDIX: SAMPLE OF PHISHING EMAIL

(No subject)

Thu 2022-09-15 20:24

1 attachments (1.85 KB)

Dr Ivan Pettersson.ppt

Good Day

I am sharing a job information to students who might be interested in a
Paid UNICEF Part-Time job to make up to $500 (USD) Weekly.

Attached is further information about the employment schedule,
if interested kindly contact Dr Ivan Pettersson with your alternative email address
(e.g yahoo, gmail, hotmail etc) and not your LDU email for urgent details of employment.

IMPORTANT NOTE: Please respond to this email via your personal email as email sent from your Duke university edu account will be disregarded. This positiion requires attention and we are using this as a test to confirm you read this email comprehensively and capable of handling this position

Regards,
Academy Career Opportunity.