Data Privacy and Cybersecurity for Higher Education Institutions

Webinar Series – Part Five

Data Privacy & Higher Education Marketing & Admissions

April 27, 2023

BOND SCHOENECK & KING ATTORNEYS

Introductions

Jane M. Sovern, Esq.
She, Her, Hers
Member – New York, NY
Higher Education Practice Group
jsovern@bsk.com | (914) 306-7826
https://www.bsk.com/people/jane-m sovern

Amber L. Lawyer, Esq., CIPP/E, CIPP/US
She, Her, Hers
Associate – Syracuse, NY
Deputy Chair – Cybersecurity and Data Privacy Practice
alawyer@bsk.com | (315) 218-8297
https://www.bsk.com/people/amber-l-lawyer

Shannon A. Knapp, Esq., CIPP/US
She, Her, Hers
Associate – Syracuse, NY
Cybersecurity and Data Privacy Practice
sknapp@bsk.com | (315) 218-8306
https://www.bsk.com/people/shannon-a-knapp

Overview

- Applicable Law
- Vendor management
- Record keeping requirements and best practices
- TCPA and alumni donations
- CAN-SPAM
- Data privacy and security in marketing and admissions
- Emerging issues

Data Privacy and Security in Marketing and Admissions

Both marketing and admissions departments routinely collect and store sensitive information from prospective students and alumni through:

- Application materials
- Medical attestations
- Financial aid forms
- Payment processing
- Alumni database websites
- Donations and fundraising campaigns

Applicable Law

- FERPA
- Title IV and GLBA Safeguards Rule
- GDPR/PIPL/ International Privacy Laws
- TCPA
- CAN-SPAM
- Data Breach Laws and Regulations

Vendor Management in Marketing & Admissions

- Higher education admissions and marketing departments routinely rely on third-party software for recruitment and alumni engagement.
- Software vendors frequently have full access to student personal information including financial information, date of birth, academic records, and more.
- Applicable law may require higher education institutions to carefully vet each vendor's ability to maintain appropriate administrative, technical, and physical safeguards to protect sensitive information.

workday. Student

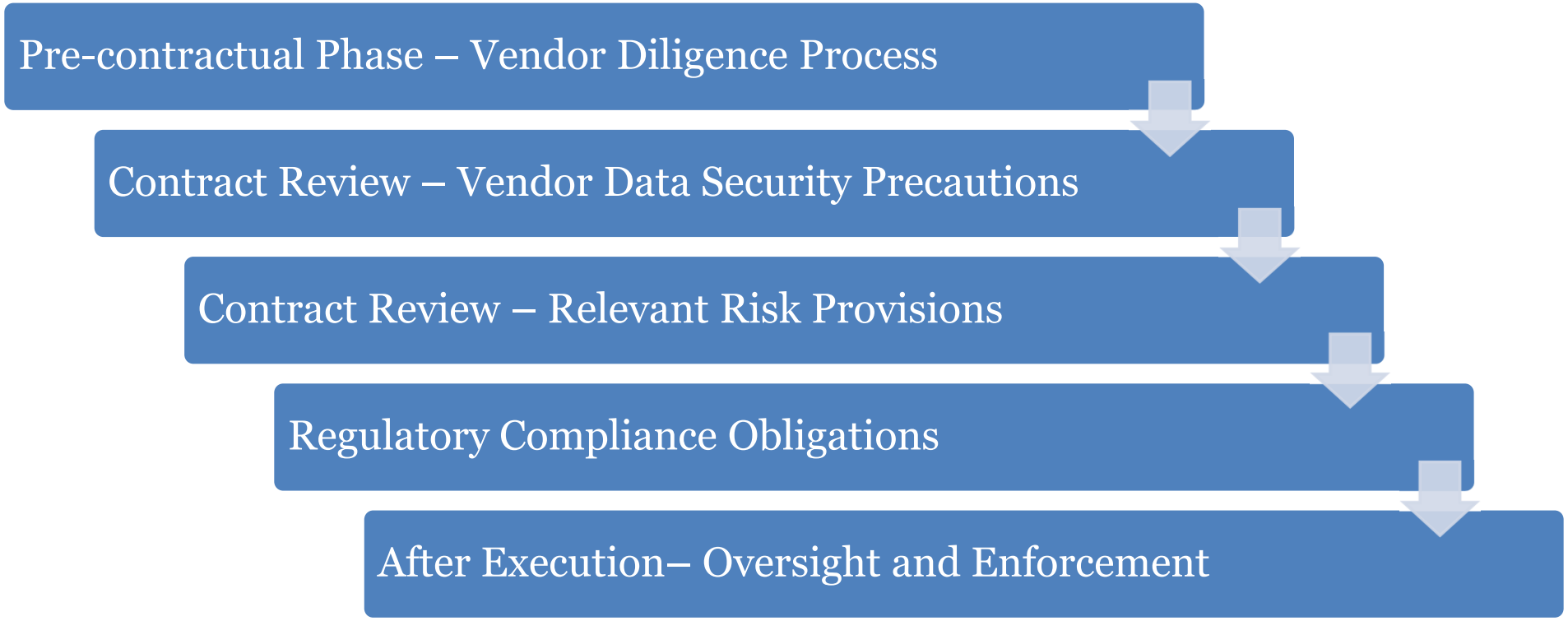
hivebrite

mailchimp

parchment recruit™

BOND SCHOENECK & KING ATTORNEYS

Risk Mitigation Strategies for Admissions and Marketing Vendors



BOND SCHOENECK & KING ATTORNEYS

Recordkeeping – Admissions

- Minimize risks by not keeping applicant data for longer than necessary
- Importance of having and following institution's records retention schedule
- Title IV Guidance
  - Generally, for three years following the end of the award year:
    - A school must keep records that substantiate the eligibility of students for FSA funds, such as: . . . **data used to establish student's admission**, enrollment status, and period of enrollment"
    - Check carefully when the 3-year period begins to run – depends on specific data

Source: https://fsapartners.ed.gov/knowledge-center/fsa-handbook/2022-2023/vol2/ch7-record-keeping-privacy-electronic-processes

Recordkeeping - Admissions

- **Common Practices for Retaining Admissions Records**:
  - For applicants who do not attend (public & private) = 2 years
  - For applicants who do enroll (private) = 5 years
  - For applicants who do enroll (public) = 6 years (See CPLR § 213)

  Based on review of Admissions Records Retention Policies at various NYS institutions of higher education

Marketing and Admissions Campaigns

- Privacy Policies
- Website Interaction
- Consent
- Telemarketing
- Text Messages

Alumni Donations – TCPA (are you a telemarketer?)

- **Telephone Consumer Protection Act** - 1991 (47 U.S.C § 227)
  - Private right of action - up to $500/violation; up to $1500/willful and knowing violation
  - Passed in wake of denial-of-service attack at Emory University in 1990
    - 10K phone extensions received recorded call; no way to disconnect
    - phone system disabled for 3 days
    - https://www.nytimes.com/1991/10/30/business/curbing-the-telephone-robots.html
  - NACUA and United Educators interpret TCPA as covering private, not-for-profit colleges

TCPA Consent – Definition and Scope

- **FCC – 2016 Declaratory Ruling (Blackboard)**
- Permits colleges to send robocalls or automated texts under two circumstances:

1) With Prior Express Consent

- Non-emergencies "closely related to the school's mission" - upcoming teacher conference or general school activity
  - Consent Definition: Student who provides phone number to educational institution gives consent "absent instructions to the contrary"

2) Without Consent

- Emergency purpose – "weather closures, fire, health risks, threats, and unexcused absences"
  - Clery Act: Timely Warnings and Emergency Notifications

https://www.fcc.gov/document/blackboardedison-tcpa-declaratory-ruling

TCPA – Marketing

- "While not squarely before us in this proceeding, reports of schools using platforms to call about ballot issues or marketing of any kind raise serious TCPA concerns." FCC Blackboard
- Franklin v. Depaul Univ., No. 16 C 8612, 2017 WL 3219253, at *1 (N.D. Ill. July 28, 2017)
- **Consent to be contacted required under TCPA for 3rd party fundraisers** (Nonprofit - written consent not required). Is giving institution phone number while a student sufficient?
- FERPA: a student's phone number is generally directory information (but check your FERPA policy's definition)

TCPA, FERPA & Alumni – Third Party Fundraisers

- **Consent not needed for alumni disclosure, but…**
  - "An educational agency or institution may disclose directory information about former students without complying with the notice and opt out conditions in paragraph (a) of this section." 34 C.F.R. § 99.37(b)
  - But what if alumnus/a opted out as a student?
  - "However, the agency or institution must continue to honor any valid request to opt out of the disclosure of directory information made while a student was in attendance unless the student rescinds the opt out request." 34 C.F.R. § 99.37(b)

CAN-SPAM

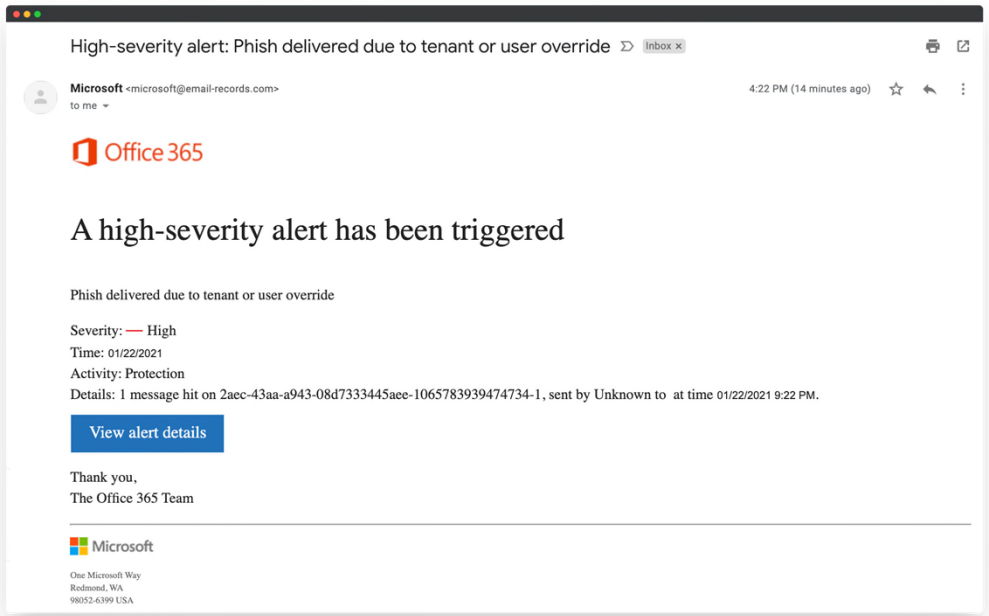
- The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)
  - Establishes requirements for those who send commercial and transactional emails
  - Provides penalties for violators and gives consumers the right to opt out of commercial email
  - Ban on false or misleading header information (an email's routing information, including the originating domain name and email address)
  - Prohibition on deceptive subject lines
  - Requirement that those who send commercial email must give recipients a free, easy-to-use opt-out method
  - Requirement that commercial email be identified as an advertisement and include the sender's valid physical postal address
  - Requirement that warning labels be added to commercial email that contains sexually oriented material

Data Privacy and Security in Marketing and Admissions

Unauthorized access to or exposure of this student information can result in liability and other negative consequences on several fronts:

- **Third Party Claims**
  - Common law negligence claims
  - Anticipated NY Privacy Act will create a private right of action
- **Regulatory Actions:**
  - NY AG levies fines for violations of the NY SHIELD Act, which includes the failure to properly notify impacted individuals
  - Depending on an impacted student's state of residency, other state AGs may also be able to levy fines
- **Business Interruption Expenses**
  - Response efforts often require IT systems to remain offline for days, sometimes weeks at a time
  - Employees may have to devote work hours to accounting for lost data and responding to stakeholder and regulator inquiries
- **Reputational Damage**
  - Ineffective and poorly implemented response efforts may result in lost public confidence, lower alumni engagement, and reduction in quality applicants
  - Numerous and repeated incidents of the same nature signals that the victim organization has not properly mitigated risks

Threats: What are Phishing/Smishing Attacks?



High-severity alert: Phish delivered due to tenant or user override Inbox ×

Microsoft <microsoft@email-records.com>
to me

4:22 PM (14 minutes ago)

Office 365

A high-severity alert has been triggered

Phish delivered due to tenant or user override

Severity: — High
Time: 01/22/2021
Activity: Protection
Details: 1 message hit on 2aec-43aa-a943-08d7333445aee-1065783939474734-1, sent by Unknown to at time 01/22/2021 9:22 PM.

View alert details

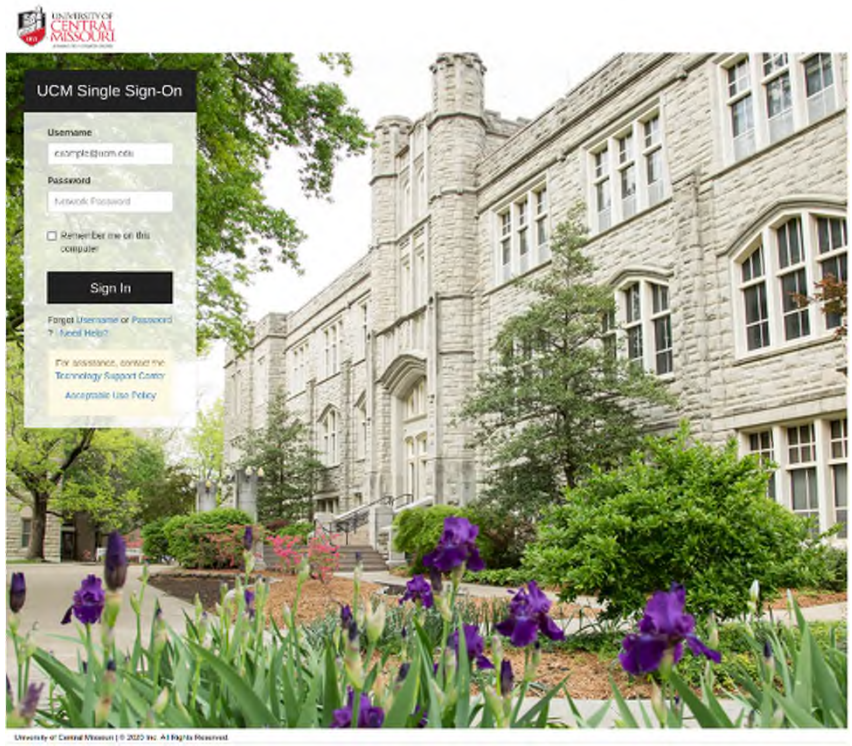
Thank you,
The Office 365 Team

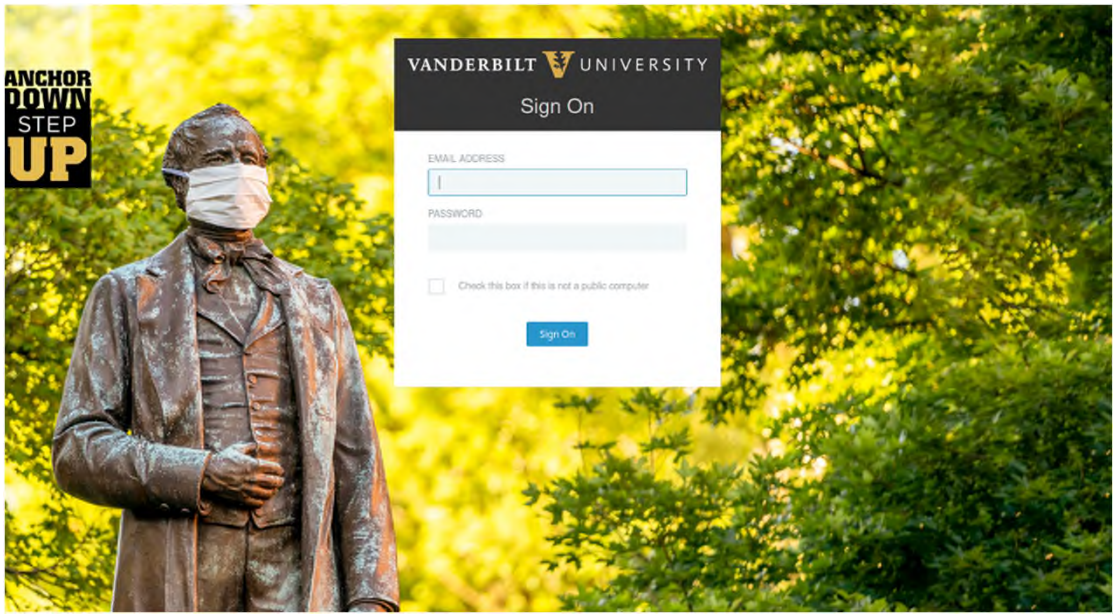
Microsoft

One Microsoft Way
Redmond, WA
98052-6399 USA

- Form of social engineering designed to deceive recipients into revealing confidential information.
- Often, emails are designed to trigger the installation of malware.
- Simpler phishing emails trick recipients into entering sensitive information like login credentials or financial information.
- Communications will typically convey a sense of urgency to pressure recipients to take action.

Phishing Attacks in Higher Ed: COVID-19





BOND SCHOENECK & KING ATTORNEYS

Phishing: Admissions and Marketing

- 2019 - University of North Texas reported a widespread phishing campaign that sent emails to prospective students titled: “Action Required FAFSA Info.”

- Other common phishing techniques in higher education:
  - Scholarship award emails
  - Alumni donation requests
  - Fraudulent job postings
  - Student and faculty account password update prompts

Admissions Breaches - FERPA

Whose records are covered by FERPA?

- **Student**
  - "any individual who is or has been in attendance at an educational . . . institution." 34 C.F.R. § 99.3. Definition of "student" includes current and former students and alumni.
  - Applicants are not "students" unless and until they are admitted and attend as students.
  - Once an applicant becomes a student, FERPA also applies to the application.

Emerging Issues to Watch

AI and Biometric Information

- Element451 - “NYU, SE Missouri State University and other schools have used a service called Element451, which rates prospects’ potential for success based on how they interact with a school’s website and respond to its messages. The result is 20 times more predictive than relying on demographics alone, the company says.”
  https://hechingerreport.org/from-admissions-to-teaching-to-grading-ai-is-infiltrating-higher-education/

- ChatGPT – Future of College Admissions Essays (Inside Higher Ed)

- UCLA case (2020) – attempted to collect Biometric Data on members of campus community

TIKTOK and IHEs

Key Takeaways

- Your employees are the first line of defense. Make sure they have access to regular trainings to help them identify potential threats.
- Your security is only as strong as your weakest sub processor. Regularly review vendor contracts, audit reports, and internal policies to ensure sub processors offer at least the same amount of protection as you do.
- Establish clear record retention schedules that align with industry best practices and applicable law.
- Ensure you have collected proper consent and develop a mechanism to track opt-outs for any phone or text outreach.

Upcoming in the Series:

Part Six: **Cybersecurity Insurance** (May 11, 2023)

By: Gail Norris, Gabe Oberfield

BOND SCHOENECK & KING ATTORNEYS

Thank You

The information in this presentation is intended as general background information.
It is not to be considered as legal advice.
Laws can change often, and information may become outdated.