A Guide to PSU Data Breach Notification Requirements

Relevant Laws

- 20 U.S.C. § 1232g; 34 CFR Part 99:
The Family Educational Rights and Privacy Act (FERPA)

- NC General Statutes Chapter 75, Article 2A:
North Carolina Identity Theft Protection Act

- NC General Statutes Chapter 115C, Article 29:
Protective Provisions & Maintenance of Student Records.

Statement on Security/Data Breach Risk Assessment: It is recommended that each impacted PSU assess the facts associated with the breach timeline to determine material risk. A security/data breach has occurred if 1) illegal use of the PII has occurred; 2) illegal use of the PII is likely to occur; or, 3) the unauthorized access to and acquisition of the PII creates a material risk of harm to an individual, then notification should be issued pursuant to NCGS 75-65.

Federal Laws Governing Student Privacy and Data Security

FERPA Definition of Student Personally Identifiable Information (20 U.S.C. § 1232g): The term includes, but is not limited to –

(a) The student's name;
(b) The name of the student's parent or other family members;
(c) The address of the student or student's family;
(d) A personal identifier, such as the student's social security number, student number, or biometric record;
(e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

FERPA Definition of Student Data Breach (20 U.S.C. § 1232g): a data breach is any instance in which there is an unauthorized release or access of PII or other information not suitable for public release. This definition applies regardless of whether an organization stores and manages its data directly or through a contractor, such as a cloud service provider. There are several breach disclosure categories to be considered and classified, including internal disclosure, external disclosure, accidental disclosure, and malicious attack. Directory information is excluded from the definition noted above.

What Type of Breach Notification Is Required Under FERPA?

FERPA requires that the agency or institution record the disclosure on the student's education record so that a parent or student will become aware of the disclosure during an inspection of said record. There is no requirement for breach notification to students under FERPA.

Important: Additional reporting requirements to the US Department of Education may apply, given the nature of the student PII available. Please seek advice from your legal counsel and/or the NC Department of Public Instruction to determine these requirements.

State of NC Laws Governing Student Privacy and Data Security

Personally Identifiable Student Data (§ 115C-402.5(a)(4a)): Student data that:

a. Includes, but is not limited to, the following:

1. Student name.
2. Name of the student's parent or other family members.
3. Address of the student or student's family.
4. Personal identifier, such as the student's Social Security number or unique student identifier.
5. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name.
6. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
7. Information requested by a person who the Department of Public Instruction or local school administrative unit reasonably believes knows the identity of the student to whom the education record relates.

b. Does not include directory information that a local board of education has provided parents with notice of and an opportunity to opt out of disclosure of that information, as provided under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, unless a parent has elected to opt out of disclosure of the directory information.

Based on the statutes noted above from § 115C-402 referencing compliance with FERPA and other relevant laws on privacy and personally identifiable information protections, it is reasonable to assume that the NC Identity Theft Protection Act and its associated requirements noted below apply to student data and extend the definition of personal information noted below to include student personally identifiable information for those populations.

North Carolina Identity Theft Protection Act of 2005 (NC General Statutes Chapter 75, Article 2A)

§ 75-61(10). "Personal information". – A person's first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records.

§ 14-113.20. Identity theft. … (b) The term "identifying information" as used in this Article includes the following:

(1) Social security or employer taxpayer identification numbers.
(2) Drivers license, State identification card, or passport numbers.
(3) Checking account numbers.
(4) Savings account numbers.
(5) Credit card numbers.
(6) Debit card numbers.
(7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).
(8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
(9) Digital signatures.
(10) Any other numbers or information that can be used to access a person's financial resources.
(11) Biometric data.
(12) Fingerprints.
(13) Passwords.
(14) Parent's legal surname prior to marriage.

§ 75-61(14) "Security breach". – An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure. defines a security breach as "the unauthorized release of unencrypted or unredacted records or data containing personal information with corresponding names, such as a person's first initial and last name."

§ 75-65. Protection from security breaches.

(a) Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. For the purposes of this section, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.

(b) Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section….

…..

(d) The notice shall be clear and conspicuous. The notice shall include a description of the following:

(1) The incident in general terms.
(2) The type of personal information that was subject to the unauthorized access and acquisition.
(3) The general acts of the business to protect the personal information from further unauthorized access.
(4) A telephone number that the person may call for further information and assistance, if one exists.
(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

(e) For purposes of this section, notice to affected persons may be provided by one of the following methods:

(1) Written notice.
(2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001.
(3) Telephonic notice provided that contact is made directly with the affected persons.
(4) Substitute notice, if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2), or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

a. E-mail notice when the business has an electronic mail address for the subject persons.
b. Conspicuous posting of the notice on the Web site page of the business, if one is maintained.

c. Notification to major statewide media.

(e1) In the event a business provides notice to an affected person pursuant to this section, the business shall notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.

(f) In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.

Application of NCGS 75-65 to Governmental Entities

§ 132-1.10. Social security numbers and other personal identifying information. … (c1) If an agency of the State or its political subdivisions, or any agent or employee of a government agency, experiences a security breach, as defined in Article 2A of Chapter 75 of the General Statutes, the agency shall comply with the requirements of G.S. 75-65. …

What Type of Breach Notification Is Required Under State of NC Laws?

NC laws require timely notice to impacted individuals who have been subject to a data breach, pursuant to § 75-65. Specifications related to the timing, distribution method, and content of said notice is outlined below.

NC 75-65 Breach Notification Requirements Checklist

(applied to PSUs by § 132-1.10 noted above)

1. Notice of breach must be given without reasonable delay, unless warranted due to law enforcement investigation.

2. Notice must be clear and conspicuous with the following items described:
    a. The incident in general terms.
    b. The type of personal information that was subject to the unauthorized access and acquisition.
    c. The general acts of the business to protect the personal information from further unauthorized access.
    d. A telephone number that the person may call for further information and assistance, if one exists.
    e. Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

3. Allowable Options for Methods of Notice:
    a. Written notice.
    b. Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically
    c. Telephonic notice provided contact is made directly with the affected persons or their guardian if minor.
    d. Substitute notice is allowed under one of the following conditions:
        i. The business demonstrates that the cost of providing notice would exceed $250,000
        ii. The affected class of subject persons to be notified exceeds 500,000
        iii. The business does not have sufficient contact information or consent to satisfy subdivisions (1), (2), or (3) of this subsection (only for those persons without sufficient contact information or consent)
        iv. If the business is unable to identify specific affected persons (only for those unidentifiable affected persons)
4. If substitute notice is selected, it must consist of all the following:
    a. E-mail notice when business has an electronic mail address for affected persons; and,
    b. Conspicuous posting of notice on website of business, if one is maintained; and,
    c. Notification to major statewide media.

5. In addition, the business shall notify the Consumer Protection Division of the Attorney General's Office of:
    a. The nature of the breach;
    b. The number of consumers affected by the breach;
    c. Steps taken to investigate the breach;
    d. Steps taken to prevent a similar breach in the future; and,
    e. Information regarding the timing, distribution, and content of the notice.

6. If notice is being provided to more than 1,000 persons at one time pursuant to this section, the business shall notify the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice.

Important: Additional reporting requirements to the US Department of Education may apply, given the nature of the student PII available. Please seek advice from your legal counsel and/or the NC Department of Public Instruction to determine these requirements.