Potential Student Data Exposure

Allison Schafer
Mon 7/25/2022 5:58 PM
To: Andrew Houlihan <Andrew.Houlihan@ucps.k12.nc.us>;Michele Morris <michele.morris@ucps.k12.nc.us>
Cc: Vanessa Wrenn

WARNING: This email originated outside of our organization.

DO NOT CLICK links or attachments unless you recognize the sender and know the content is safe.

Dear Drew and Michele:

I am writing on behalf of DPI to inform you of a potential data exposure for some of your school district's students. On July 22nd at 2:30 pm, DPI received and began investigating a report of potential student data exposure. Over the weekend and through today, the possible exposure was traced back to the vendor i-Leadr.com. Per the i-Leadr.com CEO, i-Leadr.com has a contract with the Union County Schools to provide services that involve the company having access to some of your student records.

The Joint Cyber Task Force, in collaboration with NCDPI and NC DIT, are currently working with the vendor and investigating the scope of the potential exposure and the root cause. Initial indications show the exposure has been contained; however, the teams are working to validate that no additional information is exposed on the web. Appropriate law enforcement agencies have been notified of the ongoing investigation. The vendor's CEO, Brie Beane, has indicated that she will be in contact with you.

If you have any additional questions at this time, please feel free to contact Vanessa Wrenn, DPI's Chief Information Officer at _____ . or ') (w) or me at: _____ . or (

We wanted you to have this information as soon as possible so that you can begin to take appropriate protective measures. We will be in touch with you about any further developments.

My best, as always,

Allison

Allison Schafer
General Counsel
State Board of Education
Department of Public Instruction

Follow us: Facebook, Twitter, Instagram *and* YouTube

NORTH CAROLINA
State Board of Education
Department of Public Instruction

Fwd: RtI:Stored! - Conference Call Invite

Casey Rimmer <Casey.Rimmer@ucps.k12.nc.us>
Fri 8/12/2022 4:31 PM
To: Michele Morris <michele.morris@ucps.k12.nc.us>
Not sure if you got this!

Casey Rimmer
Director of Innovation and EdTech
Teaching and Learning
Union County Public Schools

400 N. Church St,Monroe, NC 28112

704) 296-3143 Ext. 6022

www.ucps.k12.nc.us

Sent from my iPhone

Begin forwarded message:

From: Brie Beane
Date: August 12, 2022 at 3:53:04 PM EDT
Subject: RtI:Stored! - Conference Call Invite

Good afternoon,

We would like to invite you, along with your legal counsel, to join a confidential information call with our counsel regarding the current state of our investigation and findings, relevant legal considerations, the steps i-LEADR, Inc has and will be taking to ensure the ongoing security of our environment, and to address any questions and concerns you might have.

We would like to schedule this for Monday, August 15, 2022 at 3:00pm, but are sensitive to individual availability. Please let us know if this will work for you and your team, and we will circulate an invite on Monday morning unless we cannot gather a critical mass. We again thank you for your patience as we have worked on these matters, and we remain available should you have any questions or concerns.

Thank you,
Brie

--

Brie Beane M.Ed.
President at i-LEADR, Inc.

A | 211 South Center Street Suite 309
Statesville NC 28677
P | 704-275-5350 ext. 1000
W | www.i-LEADR.com

RE: Contact emails for the district and school attorneys for I-Leadr clients

James Paulino
Thu 8/25/2022 3:34 PM

To: Allison Schafer >;Dean Shatley ;Michele Morris <michele.morris@ucps.k12.nc.us>;Eva Dubuisson >;Melissa Michaud m>;Whitley Ward >;Ed Ritter

Cc: James Paulino >;Julien AlHour >;Vanessa Wrenn Susan Fuster-Marin >;Paolo Shipman

WARNING: This email originated outside of our organization.

DO NOT CLICK links or attachments unless you recognize the sender and know the content is safe.

Allison,

Thank you for providing so quickly.

Best,
Jimmy

James Paulino
Partner
Mullen Coughlin LLC
75 S Clinton Ave Suite 510
Rochester, NY 14604
(267) 930-4741 - Office

https://www.mullen.law/

From: Allison Schafer
Sent: Thursday, August 25, 2022 3:33 PM
To: Dean Shatley ; Michele Morris <michele.morris@ucps.k12.nc.us>; Eva Dubuisson ; Melissa Michaud ; Whitley Ward ; Ed Ritter
Cc: James Paulino ; Julien AlHour ; Vanessa Wrenn
Subject: FW: Contact emails for the district and school attorneys for I-Leadr clients
Importance: High

All, below is the information you requested yesterday about the requirements for approving third party integrations with the state systems. Please let us know if you have any questions or need any further information. My best, Allison

Allison Schafer
General Counsel
State Board of Education
Department of Public Instruction

Follow us: Facebook, Twitter, Instagram *and* YouTube

NORTH CAROLINA
State Board of Education
Department of Public Instruction

From: Julien AlHour
Sent: Thursday, August 25, 2022 2:38 PM
To: Allison Schafer
Cc: Vanessa Wrenn
Subject: Re: Contact emails for the district and school attorneys for I-Leadr clients
Importance: High

Corrected the VRAR link. The previous one was dead.

Julien Alhour
Director
Office of Enterprise Systems

Division of Digital Learning and Technology Services

Follow us: Facebook, Twitter, Instagram, and YouTube

North Carolina Department of
PUBLIC INSTRUCTION

From: Julien AlHou
Sent: Thursday, August 25, 2022 2:28 PM
To: Allison Schafer <
Cc: Vanessa Wrenn <
Subject: Re: Contact emails for the district and school attorneys for I-Leadr clients

Hello Allison,

The security requirements for approving 3rd party integration with state systems are listed below. We are considering simplifying the VRAR for the PSUs. But, as it stands now, we are using this VRAR from. Please share with the Attorney's. We are working on a memo to go out to the PSUs regarding the revalidation of existing integrations and further clarify the process for requesting such integrations. Please feel free to share this information with the lawyers who asked for it.

1. A Vendor Readiness Assessment Report (VRAR): https://it.nc.gov/documents/files/vendor-readiness-assessment-report-non-state-hosted-solutions/open --as the name suggests, this is a self-assessment to be completed by the vendor to capture their baseline security controls in accordance with NIST 800-53 -- the framework that our State security policies are derived from. This is normally required just once at the start of any State-vendor relationship.

2. A recent (valid within the last 12 months) favorable third-party attestation (SOC 2 Type 2) or audit certification (ISO 27001) or FedRAMP Authorization for the SaaS environment in scope. This serves as independent verification that a comprehensive information security program is in place. **An updated report is required annually.**

3. To provide assurance of continuous monitoring, diagnostics, and mitigation, we ask for:
    a. A penetration test report (dated within the last 12-months) of the application(s) and environment(s) in scope. We request that this comes from a third-party. **An updated report is required annually.**
    b. A scan report (dated within the last 30-days) demonstrating internal credentialed vulnerability scanning of the application(s) and environment(s) in scope. **An updated report is required annually.**
    c.
4. We require these artifacts and any findings from within to be remediated in accordance with State security requirements, prior to the start of data sharing.

Best,

Julien Alhour
Director
Office of Enterprise Systems
Division of Digital Learning and Technology Services

Follow us: Facebook, Twitter, Instagram, and YouTube

North Carolina Department of
PUBLIC INSTRUCTION

From: Allison Schafer <
Sent: Thursday, August 25, 2022 2:05 PM
To: Julien AlHour <
Subject: Fwd: Contact emails for the district and school attorneys for I-Leadr clients

Julien,

Can you please send the requested information to me and I will send it in to Mr. Paulino? Thanks

Allison.

Get Outlook for iOS

From: James Paulino >
Sent: Thursday, August 25, 2022 12:30:29 PM
To: Allison Schafe
Cc: James Paulino >; Susan Fuster-Marin ; Paolo Shipman

Subject: RE: Contact emails for the district and school attorneys for I-Leadr clients

Good afternoon, Allison,

I wanted to touch base regarding (I think) the "bulletin 18" referenced by Julian (?) on yesterday's call outlining the State's security requirements. We have received inquiries regarding the effort to confirm security, and we have put our penetration testing on hold until we obtain the state requirements. We've tried to find anything on the DPI website about this, and are not seeing it, and it seemed that Julian was saying that these are not public?

Any thoughts on when we might expect to receive?

Thoughts?

Thank you,
Jimmy

James Paulino
Partner
Mullen Coughlin LLC
75 S Clinton Ave Suite 510
Rochester, NY 14604
(267) 930-4741 - Office

https://www.mullen.law/

From: Allison Schafer
Sent: Wednesday, August 24, 2022 6:12 PM
To: James Paulino >; Michele Morris <michele.morris@ucps.k12.nc.us>; Eva Dubuisson

Melissa Michaud <[redacted]>;
max@garnerwilliamson.com; David R. Hostetler, Esq. <[redacted]>; Whitley Ward
<[redacted]>; Ed Ritter <[redacted]>
Cc: Dean Shatley <[redacted]>
Subject: Contact emails for the district and school attorneys for I-Leadr clients

Jimmy, below is the list of the school attorneys and one non-attorney contact for the I-Leadr Clients. I am also copying them all on this email. I hope this provides you with what you need. Thanks for participating in the call today. I think it was best to get everyone together. I beleive it was helpful. Hopefully we are closer to getting through this. My best, Allison

Dean Shatley
Campbell Shatley law firm, Asheville NC

Representing 3 school districts;
Iredell-Statesville
Newton-Conover
Stanley County

Michele Morris, In house counsel
michele.morris@ucpsk12.nc.us
Representing Union County Schools

Eva DeBubuisson and
Melissa Michaud
Tharrington Smith law firm, Raleigh, NC

Representing 3 school districts:
Granville County
Person County
Warren County

Max Garner
Garner Williamson law firm, Troy, NC

Representing the Montgomery County Schools

David Hostetler
Lex-is School Law Services, Durham, NC

Representing Piedmont Community Charter School

Whitley Ward
The Womble Law Firm, Elizabethtown, NC

Representing the Emereau Bladen Charter School

Ed Ritter
Vice Chair of the Board of Directors of
Veritas Community Charter School

(Mr. Ritter is the contact person – the School has not retained an attorney)

Allison Schafer
General Counsel
State Board of Education
Department of Public Instruction

Follow us: Facebook, Twitter, Instagram *and* YouTube

NORTH CAROLINA
State Board of Education
Department of Public Instruction

Visit us on the web at https://dpi.nc.gov . All e-mail correspondence to and from this address is subject to the

North Carolina Public Records Law, which may result in monitoring and disclosure to third parties, including law enforcement.

Visit us on the web at https://dpi.nc.gov . All e-mail correspondence to and from this address is subject to the North Carolina Public Records Law, which may result in monitoring and disclosure to third parties, including law enforcement.

Visit us on the web at https://dpi.nc.gov . All e-mail correspondence to and from this address is subject to the North Carolina Public Records Law, which may result in monitoring and disclosure to third parties, including law enforcement.

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.

Disclaimer: *The information contained within this document is offered as an educational and reference tool and does not constitute legal advice or guidance.*
Please consult your own legal counsel to determine the best course of action for your own PSU.

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.