NORTHERN ILLINOIS UNIVERSITY
Ethics and Compliance Office

Hon. Kwame Raoul - Office of the Illinois Attorney General
databreach@ilag.gov

Mr. John Hollman - Clerk of the Illinois House of Representatives
Mr. Tim Anderson - Secretary of the Illinois Senate
Reports@ilga.gov

December 13, 2024

Dear Colleagues:

Pursuant to the Illinois' Personal Information Protection Act (815 ILCS 530/1 *et. seq.*), Northern Illinois University ("the University") is submitting this annual report listing all breaches of the security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.

During calendar year 2024, the University reported one (1) breach to the Attorney General and General Assembly. The attached letter, dated June 10, 2024, provides an explanation of the phishing scam involved and corresponding corrective measures, which includes notification of the affected individuals, investigating other unauthorized access (which was not found), reminding of obligations under information security training and removing certain sensitive information from the self-service portal.

Please contact the undersigned with any questions or comments you may have.

Thank you,

Sarah Garner
Ethics and Compliance Officer
Northern Illinois University
sadamski1@niu.edu,
815-753-5560

Enclosure

CC: Bob Barton, Director of Information Security, Northern Illinois University
Gregory Brady, Deputy General Counsel, Northern Illinois University

NORTHERN ILLINOIS UNIVERSITY
Ethics and Compliance Office

Hon. Kwame Raoul - Office of the Illinois Attorney General
databreach@ilag.gov

Mr. John Hollman - Clerk of the Illinois House of Representatives
Mr. Tim Anderson - Secretary of the Illinois Senate
Reports@ilga.gov

June 10, 2024

To whom it may concern,

Northern Illinois University ("the University") is providing this report pursuant to Illinois' Personal Information Protection Act (815 ILCS 530/1 *et. seq.*), of an act of unauthorized acquisition of personal information of Illinois residents.

The University has become aware of three incidents in which *phishing* scams led to unauthorized access to the personal information of student employees. The breaches occurred through the following methodology: the student employees received an email to their University-provided account "requesting" or "requiring" they change their passwords in the University Human Resources (HR) self-service portal. The three student employees followed the links and changed their personal passwords, erroneously confirmed accesses to the accounts via the University's multi-factor authentication (MFA) system(s) and, as a result, outside bad actors gained access to only their individual HR portals.

As a result, the three student employees' direct deposit authorizations were diverted to a third-party account for one pay cycle. The issue was caught immediately, isolated and remedied. Other than direct deposit information, access to these accounts may have exposed the student employees' directory information and Social Security numbers. Those affected have been appropriately notified.

The University investigated to ensure that no other unauthorized access was permitted, either in their personal accounts or to wider University or third-party software information storage, and none was allowed.

The University already provides information security training to employees, and the individuals were reminded of the obligations they have. This was not a system-wide issue, and does not indicate broader level issues with security, either in process or policy. We had already begun the

process of removing access to Social Security numbers in the self-service portal, such as removing them from available tax forms.

The University will further update you should additional relevant information become available. Please feel free to contact the undersigned with any questions or comments you may have.

Jack Yetter
Director of Privacy/Privacy Officer
jyetter@niu.edu
815-753-1682