-- New York State Office of the Attorney General -

NEW YORK STATE SECURITY BREACH REPORTING FORM

Pursuant to the Information Security Breach and Notification Act (State Technology Law §208)

Name and address of Entity that owns or licenses the computerized data that was subject to the breach:
State University of New York at New Paltz
Street Address: 1 Hawk Drive
City: New Paltz State: NY Zip Code: 12561

Submitted by: Paul Chauvet Title: Information Security Officer Dated: February 26th, 2020
Firm Name (if other than entity): ______________________________
Telephone: [redacted] Email: [redacted]@newpaltz.edu
Relationship to Entity whose information was compromised: ______________________________

Type of Organization (please select one): [X] Governmental Entity in New York State; [ ] Other Governmental Entity; [ ] Educational; [ ]Health Care; [ ]Financial Services; [ ]Other Commercial; [ ]Not-for-profit

Number of Persons Affected:
Total (Including NYS residents):_~125 NYS Residents: Uncertain percentage of which are NYS residents yet
If the number of NYS residents exceeds 5,000, have the consumer reporting agencies been notified? [ ] Yes; [ ] No.

Dates: Breach Occurred: 1/15 through 2/26 Breach Discovered: 2/25 Consumer Notification: 2/26

Description of Breach (please select all that apply):
[ ]Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape);
[ ]Internal system breach; [ ]Insider wrongdoing; [ ]External system breach (e.g., hacking); [ ]Inadvertent disclosure;
[X]Other (specify): Student Accounts compromised via phishing

Information Acquired: Name or other personal identifier in combination with (please select all that apply):
[ ]Social Security Number
[ ]Driver's license number or non-driver identification card number
[ ]Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account
Potentially grade information, address/phone numbers, and tuition bill information. SSN or bank accounts not compromised

Manner of Notification to Affected Persons - ATTACH A COPY OF THE TEMPLATE OF THE NOTICE TO AFFECTED NYS RESIDENTS:
[ ] Written; [ ] Electronic; [ ] Telephone; [ ] Substitute notice.
List dates of any previous (within 12 months) breach notifications: ______________________________

Identify Theft Protection Service Offered: [ ] Yes; [X] No.
Duration: ______________ Provider: ______________________________
Brief Description of Service: ______________________________

Details below on what we have found

Yesterday, February 25th, an electronic refund was attempted to be disbursed to a student. That deposit was rejected since the destination account was frozen. That led the college to investigate further where we found the following in our payment processor (Cashnet)

- There were over 120 student accounts which had their direct deposit information for their loan disbursement refund updated to suspicious accounts. This included:
    - 80 student refunds had their refund bank account destination changed to a single bank account (name: [redacted])
    - 32 student refunds had their refund bank account destination changed to a second account (name: [redacted])
    - 10 student refunds had their refund bank account destination changed to a second account (name: [redacted])
- The time frame for these changes was during the past month or so (2 changes on January 15th, the rest between February 4th and today)
- Only a small fraction of refunds were actually sent out to these suspicious accounts (7 students - $10,210.57 disbursed).
- We are reasonably certain that these accounts were compromised due to phishing. Three student accounts were compromised and used to send fraudulent phishing emails to students/faculty/staff (on January 7th, February 4th, February 16th, and today February 25th).

Current mitigation steps:

- We have disabled e-refunds until we have two-factor authentication in place to protect student accounts. Until then – we are using paper checks (disbursed in-person to students, or mailed out to verified mailing addresses)
- We are disabling the affected student's computer accounts until they can visit our Service Desk in-person (or call and verify their identity) to change their passwords.
- We are investigating what other access may have been made by these compromised accounts.
- We have engaged our University Police in this investigation – and they are contacting the FBI.

Future mitigation steps

- Prior to this – we already had plans to implement multi-factor authentication for all students. We have already done this for all employees in 2019. We will be accelerating these plans. Until MFA is implemented for all students – we do not plan on re-enabling electronic refunds.
- We are looking to expand our information security awareness training to include all students (not just employees).