CHIEF PRIVACY OFFICER'S 2020 ANNUAL REPORT ON DATA PRIVACY AND SECURITY

Pursuant to NYS Education Law §2-d, the Education Department's Chief Privacy Officer is required to issue an annual report on:

(1) data privacy and security activities and progress,
(2) the number and disposition of reported breaches, if any, and
(3) a summary of any complaints of possible breaches of student data or teacher or principal annual professional performance review data (PII).

This report covers the reporting period of January 1 to December 31, 2020.

I. Summary of Data Privacy and Security Activities and Progress

The COVID-19 pandemic made 2020 a challenging year for the entire world and the education sector was no exception. School closures caused districts to increasingly rely on technology platforms to deliver education. This increased digital footprint required increased vigilance in the areas of data protection and cybersecurity. The work the privacy office has been doing with districts since 2017 paid off, as districts were able to quickly pivot to remote learning while taking steps to protect personally identifiable information. To aid this work, my office issued guidance and model terms and conditions to help districts as they negotiated contracts with technology vendors to implement the shift to remote learning.

While the education sector remained a target for cybercriminals, there was a decrease in reported incidents of ransomware; additionally, reported attacks on school districts and other educational agencies were less severe than in previous years. The number of reported ransomware incidents decreased from 16 in 2019 to 10 in 2020. My office coordinated responses to the incidents with the affected educational agencies, the NYS Office of Information Technology Services, state

III. Summary of Incidents Reported by Educational Agencies that Implicated Student PII

#	Description
1	A student, in response to a challenge, accessed the school network and obtained a file containing student network login information
2	Ransomware.
3	Ransomware.
4	School staff sent a report containing student PII to the wrong parent.
5	Student accessed a file containing student PII because access to the file was not properly restricted.
6	School district erroneously sent an email containing a file of 66 student records that included, among other things, student transcripts, names and addresses to one student.
7	School support staff, in preparation for a parent meeting, sent student PII to the wrong parents.
8	Ransomware.
9	Ransomware.
10	A teacher's twitter pw 11.528.5r (s)-4.3 (t)-5. 4 (i)-3.6 (n)-0.c(6)o 006 Tw 18P /MCID 35 BDC 460.8(r)-2..3 (p

31