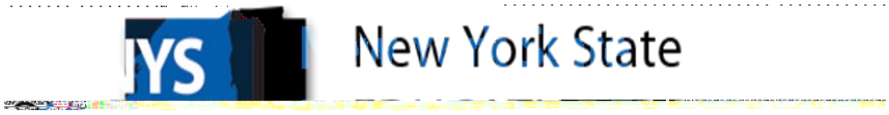
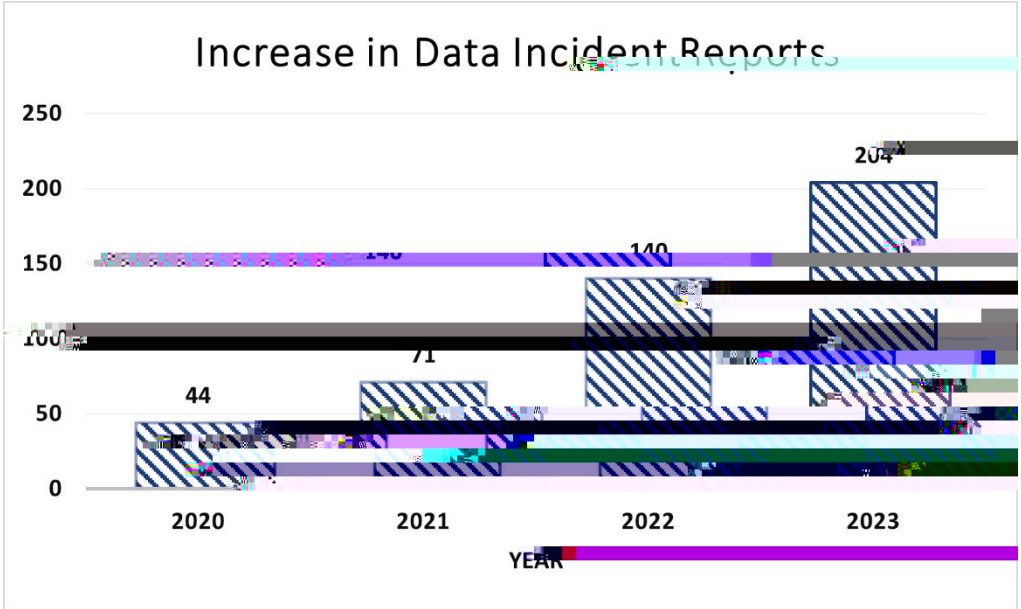


CHIEF PRIVACY OFFICER'S 2023 ANNUAL REPORT

As in previous years, 2023 saw a continued increase in reported data incidents. Reports to the Privacy Office have grown from 44 (2020) to 71 (2021), to 140 (2022), and now 204 in 2023. As in 2022, most incidents reported to the Privacy Office arose from human error, typically the inadvertent transmission of information to an unrelated party via email or attachment. Section II of this report includes examples of the types of human error breaches.

Additionally, approximately 30 percent of this year's incidents (60 incidents) involved 17 different third-party contractors or vendors. Furthermore, 2023's incidents reveal that phishing attacks are increasing in number and that educational agency staff continue to fall prey to them. Educational agencies must ensure that their staff are properly prepared for these increasingly sophisticated phishing attacks.



The Privacy Office has multiple goals for 2024, including:

1) Continuing to engage with internal and external stakeholders, particularly superintendents, charter schools and State-approved special education schools.
2) Working with the Regional Information Centers (RICs) to offer student data privacy consortium memberships for school year 2024-2025. The State's membership in Access for Learning (A4l) and the RICs' membership in The Educational Cooperative (TEC) will assist educational agencies with drafting, negotiating, and managing Data Protection Agreements (DPAs) for third-party contractors and vendors.
3) Developing an on-line form for human error data incidents. As the number of data incidents increase each year,[3] the Privacy Office will be seeking to implement an easier method to report and track human error incidents.
4) Review Part 121 of the Commissioner's regulations with the goal of offering proposed amendments. At a minimum, the regulations need to be amended to change the reference to the National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 to the recently released Version 2. This presents an opportunity to consider whether other aspects of Part 121 should be amended.

Sections II and III of this report analyze and describe reported breaches. This summary includes the disposition of data incident report filings. Section IV of this report summarizes complaints concerning possible breaches of student or certain teacher/principal data during 2023 and the Privacy Office's disposition thereof. As indicated above, this year's report contains a new Section V, which reports the results of the Privacy Office's 2023 monitoring of educational agencies' web sites for compliance with FERPA, Education Law § 2-d and Part 121 of the Commissioner's regulations.

The Privacy Office looks forward to continued collaboration with our external stakeholders: school districts, charter schools, State-approved special education schools, Boards of Cooperative Educational Services (BOCES) and Regional Information Centers (RICs), parents and advocates as well as our internal stakeholders at NYSED, as we continue to provide guidance about the legal and regulatory requirements and importance of data privacy and security.

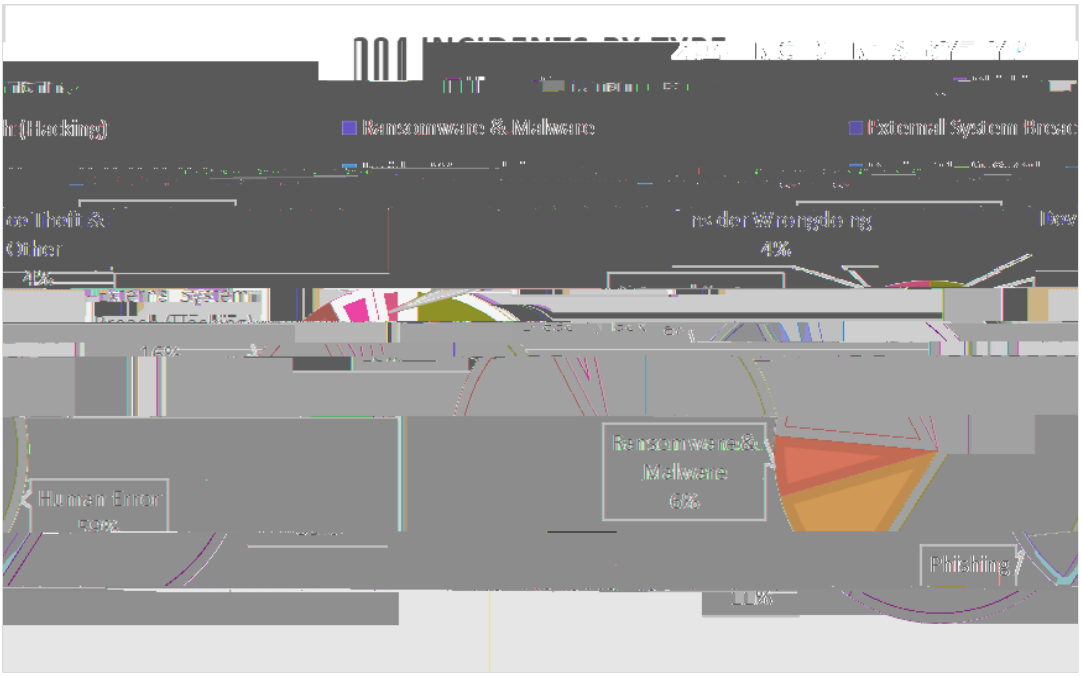
Finally, I must acknowledge my tireless staff without whose assistance this report would not be possible, but also for their committed work in an often-overwhelming environment. They are both truly dedicated to the issue of student privacy.

Louise DeCandia
Chief Privacy Officer

[3] As of mid-February, the Privacy Office has already received more than 150 data incident reports for 2024.

II. Reported Breaches 2023

In 2023, the Privacy Office received 204 data incident reports from 113 different educational agencies, a 31 percent increase from the 140 incidents reported in 2022. Of these 204 incidents, 121 were due to human error, 23 to phishing attacks, 32 to an external breach or hacking, 12 to ransomware and malware attacks, 9 to insider wrongdoing, and 7 to other incidents such as theft of a device. These breakdowns by percentages, can be viewed in the chart below.



Human error accounted for 121 of the 204 incident reports. As seen in the chart below, human error led to 109 unauthorized disclosures and 12 unauthorized access incidents. Many of these incidents resulted in the unauthorized disclosure of Personally Identifiable Information (PII) through email. There were also several incidents of misconfigured on-line forms that allowed people to see, for example, complaints filed online by parents or students including PII. These reports and parent complaints led to specific guidance issued by the Privacy Office in July to address online compliant or submission forms.

Distributions of Incidents Due to Human Error

- A substitute teacher provided their username and password to a student, allowing the student to have unauthorized teacher-level access to the school's portal for approximately four months until discovery by the school.
- An educational agency reported that a staff member and student reviewed the students' profile in a student information management system (Infinite Campus). The student and staff member also viewed another student's profile. Thereafter, the student reviewed other students' PII.
- A high school student, the child of a school employee, used their parent's credentials to log in and view a classmate's medical information to confirm a rumor regarding the classmate's diagnosis.
- A guidance counselor asked their student assistant to help issue "promotion in doubt" letters to fellow students.

Around 29 percent of the incidents reported in 2023 (60 incidents) involved approximately 15 third-party contractors or vendors. Some of the reports filed were never verified and there was no evidence of a breach. This was the case with a therapy company located downstate that was investigated by the Privacy Office. That matter shed light on the importance of obtaining evidence of a breach/unauthorized access before sharing such information with other educational agencies. Examples of third-party contractor or vendor incidents include:

- Several institutes of higher education[5] reported a data breach by National Student Clearinghouse (NSC). NSC is an organization that NYSED contracts with to match high school graduates with students enrolled in postsecondary education. Although NSC was subject to the MOVEit breach,[6] New York's data was not affected. The Privacy Office followed up with SUNY System Administration, which confirmed that its data was similarly unaffected.
- The New York City Department of Education was affected by the MOVEit breach as well as a breach of data held by Kirkland & Ellis, the law firm representing Illuminate Education (now Renaissance Learning). The Kirkland & Ellis breach caused thousands of New York families to be notified again that their children's data was breached.[7]
- One educational agency reported that ClassLink inadvertently moved the school's database to Bozeman, Montana, affecting the data of 240 students.

---

[5] Colleges, Universities, and Institutions of Higher Education are not educational agencies or schools within the definitions in Education Law 2-d and therefore are not required to report breaches to NYSED's Privacy Office.

[6] MOVEit is a secure file transfer program owned by Progress Software. In May 2023 a group called CLOP

- Sphero, a STEM education product, suffered a data breach that was reported by five school districts and two BOCES contract consortiums. With few exceptions, the only student data that was breached were names; many schools had no data breached.

The Privacy Office received 23 data incident reports pertaining to phishing attacks.

- Several schools received a phishing attack sent to student and employees with the subject line "looking for work."
- Eight educational agencies reported a phishing attack on a third-party vendor that provides therapy services.
- Several schools reported receipt of a phishing email using NYSED's logo and identification. Although the email did not originate with NYSED, the agency's IT staff were able to stop the emails.
- A clerk employed by an educational agency notified their Director of Technology that they responded to a phishing email attack while they were out of the office. When questioned as to why the clerk logged in while out of the office, the clerk admitted leaving their username and password on a card located on their desk to share with another staff member.
- In several circumstances, school staff were able to prevent harm from a phishing attack because staff promptly reported the incident.

<u>Cyberattacks</u>

New York's educational agencies suffered approximately 40 cyberattacks during 2023. Of these, eight incidents were reported at the end of August and beginning of September. Data shows that many cyberattacks occur just before the new school year begins and during school breaks.

- One educational agency had more than 44,000 records affected. Some of these records went back to 1950.
- In one educational agency, a student's Google email account was hijacked. The account was used to send emails to other students and staff but only one student opened the phishing email.
- At least two educational agencies were subject to Google directory scraping from an unknown third-party.

Office, the educational agency is often asked to provide a detailed investigation report. The Privacy Office strives to render timely[8] decisions that assist educational agencies and complainants in understanding the laws, regulations and requirements pertaining to student, teacher and principal data privacy and security. Additional investigation may be undertaken directly by the Privacy Office.

In 2023 the Privacy Office received 31 complaints that resulted in 14 written determinations.[9]

student data, or that any breach occurred. However, it was determined that the employee should have informed the former employer

school's required form—and, if so, when the school received a copy thereof—the Privacy Office could not determine that the posting of the photograph constituted an unauthorized disclosure.

6. Cohoes City School District (issued 7/13/23):

A parent asserted, first, that their school district improperly denied their request to access their child's records and, second, allegedly disclosed PII without consent. With respect to access, the school district denied the request because it was unable to verify that the person requesting the inspection of the student's records was, in fact, a parent. Regarding the inadvertent disclosure, the school admitted that its attendance officer improperly solicited information concerning the student's residency with a landlord in connection with a residency investigation. However, it was not clear if the outreach resulted in the disclosure of the student's PII. In sum, the Privacy Office was unable to find that the school disclosed the student's PII in violation of FERPA and/or Education Law § 2-d.

11. Lackawanna City School District (issued 4/7/23):

A parent complained that completed online forms for reporting violations of the Dignity for All Students Act remained accessible for viewing by other students. The school district acknowledged that its form, modified sometime in November or December of 2022, was not adequately reviewed before being posted to the school district's web page. This caused completed forms to remain publicly available after being completed by a parent or student. While the school district immediately corrected the problem, the Privacy Office required it to determine the exact date of modification so that it could notify all families who filed out the form prior to that date.

12. Saugerties Central School District (issued 8/16/23):

A parent asserted that an employee of the school district inappropriately disclosed their child's PII to their former spouse. The school district acknowledged the improper disclosure, explaining that an employee received a note from the complaining parent regarding the students' pickup and then forwarded the information to the students' other parent, with whom the employee has a personal relationship. The school district was reminded: (1) to use reasonable methods to ensure that school officials only obtain access to education records in which they have a legitimate educational interest; (2) to conduct annual privacy trainings; and (3) inform school staff of the inappropriateness of sharing observations and personal knowledge about students obtained in their roles as school district employees.

13. Success Academy Rockaway Park Middle School (issued 12/21/23):

A parent asserted that a charter school improperly disclosed their child's PII when it posted all the students' GPAs in a manner visible to everyone entering the student's classroom. The Privacy Office determined that the charter school's practice of disclosing and sharing student GPAs violated FERPA and constituted an unauthorized release or disclosure under State regulations. The charter school was directed to revise its policies and obtain the express written consent of parents, guardians or eligible students before engaging in such practice.

that it does obtain parent consent and does not rely on a directory information policy to share this information. The determination is under review.

14. Wappingers Falls CSD (issued 12/13/23):

A parent argued that the school district improperly disclosed her child's PII when its transportation department was notified that the student did not need to be picked-up for several days due to a suspension. The school district admitted that it provided such information to two employees. It asserted that the employees had a legitimate educational interest in this information because the students' absence impacted the school's transportation schedule. The Privacy Office agreed that the school district had a legitimate educational interest in sharing information with the transportation department regarding student availability for pick-up and drop-off. While the parent's concern was valid, there was no evidence that the school district shared the student's information for improper reasons.

V. Monitoring of Educational Agencies' Web Sites

As contemplated in last year's annual report, the Privacy Office developed a monitoring initiative of educational agencies for compliance with FERPA, Education Law § 2-d and Part 121 of the Commissioner of Education's regulations. In July 2023, I sent a memorandum to the field explaining what information the Privacy Office would be monitoring in the fall. The memorandum listed nine school districts that have model privacy web pages. During September and October, 120 educational agencies websites, including those of five charter schools, were monitored for the following:

- FERPA Annual Notification to Parents;
- Directory Information Policy;
- Education Law Section 2-d and 121.3(a): Parents' Bill of Rights (PBOR);
- Education Law Section 2-d and 121.4: Information on how parents can file a complaint;
- Education Law Section 2-d and 121.3(d): supplemental information to the PBOR for any contract or other written agreement with a third-party contractor that will receive personally identifiable information, and
- Education Law Section 2-d and 121.5(b): data security and privacy policy that implements the requirements of Part 121 and aligns with the NIST Cyber Security Framework (CSF).

Educational agencies were also encouraged to maintain a page on their websites devoted to privacy requirements, making data privacy and security information easily accessible, and transparent, to parents and eligible students. After monitoring by the Privacy Office, all