CHIEF PRIVACY OFFICER'S 2023 ANNUAL REPORT ON DATA PRIVACY AND SECURITY

Pursuant to Education Law § 2-d, the New York State Education Department's (NYSED) 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 (APPR) data.

This report addresses the reporting period of January 1 to December 31, 2023.

I. Opening and Summary of Data Privacy and Security Activities and Progress

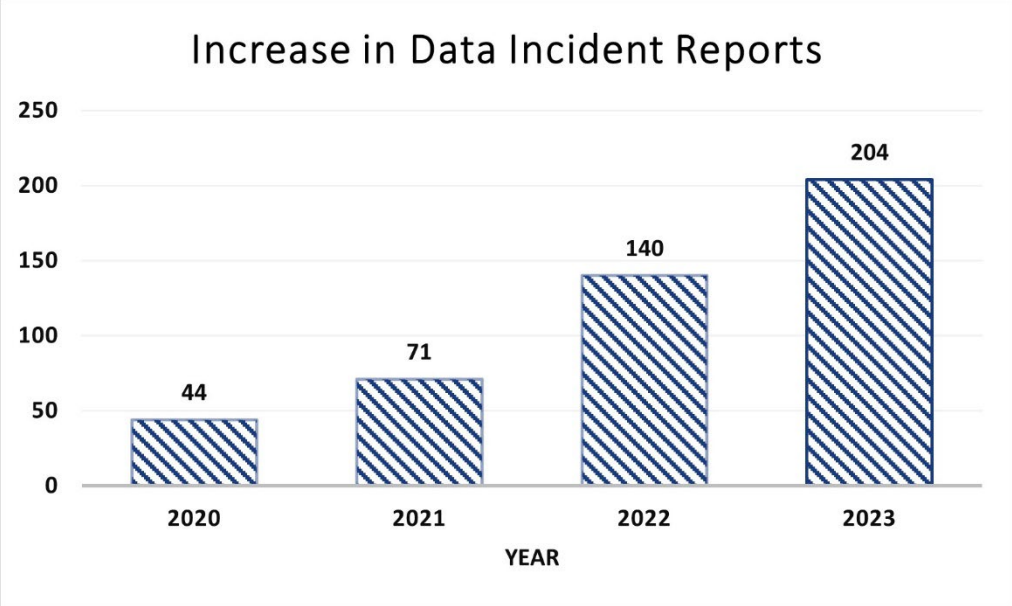
Part 121 of the Commissioner's regulations, which implement Education Law § 2-d, require educational agencies[1] to report "every discovery or report of a breach or unauthorized release of student, teacher or principal data" to my office no more than 10 calendar days after such discovery [§ 121.10 (d)]. A breach is broadly defined to mean "any unauthorized acquisition, access, use or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use or receive the student data or the teacher and/or principal data." [§ 121.1 (a)]. Unauthorized disclosure or release is defined as "any disclosure or release" not permitted/authorized by: (1) federal or State statute or regulation; (2) a lawful contract or written agreement, or (3) a lawful order, including those issued by a court or tribunal [§ 121.1 (t)].

These regulations require reporting of any unauthorized release of student data or teacher and/or principal APPR data to the Privacy Office whether or not there is evidence that the data was accessed. Some of the incident reports the Privacy Office received in 2023 demonstrate that educational agencies remain uncertain as to when they are required to report an incident. Any educational agency that has questions regarding the reporting requirements should contact NYSED's Privacy Office privacy@nysed.gov.

[1] Education Law § 2-d defines educational agency as a school district, board of cooperative educational services (BOCES), school or NYSED. Schools are defined to include charter schools.

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.



In addition to the increase in data incident reports, the Privacy Office saw a substantial increase in privacy complaints. The Privacy Office received 31 complaints that resulted in 14 written determinations.[2] Of the 16 additional complaints, 11 parents received a letter explaining why the Privacy Office was unable to render a determination. Section IV of this report contains a more detailed description of the complaint determinations.

The Privacy Office completed the monitoring described in the 2022 Annual Report. The results of this monitoring are described in Section V.

[2] An additional 16 complaints were reviewed or investigated by the Privacy Office but did not result in final determinations. One complaint filed in 2023 will be issued in 2024.

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 (A4I) 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.

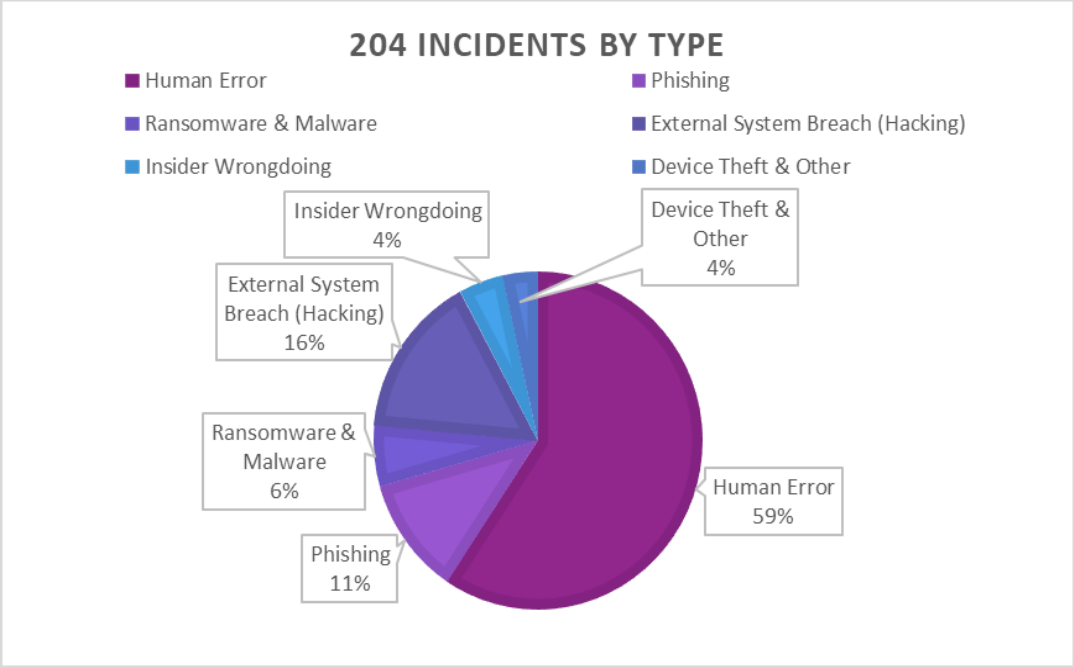
Finally, I must acknowledge my tireless staff without whose assistance this report would not be possible, but also for their committed work in an often-overwhelming environment. They are both truly dedicated to the issue of student privacy.

Louise DeCandia
Chief Privacy Officer

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

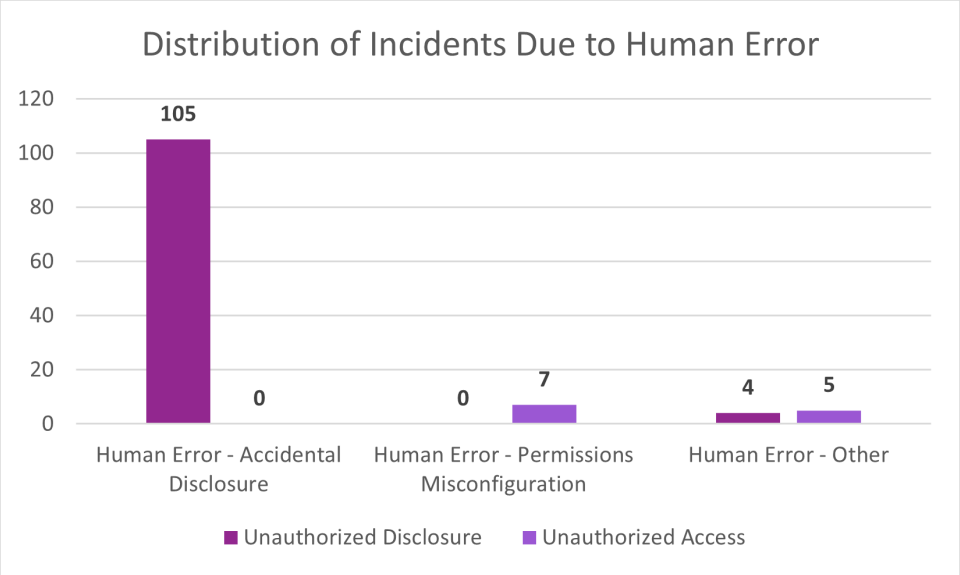
II. Reported Breaches 2023

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 and Unauthorized Disclosures

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.



Examples of human error caused breaches are:

- An email intended only for all school district principals was sent to all school district staff.
- A response to a Freedom of Information Law (FOIL) request was unredacted and included PII.
- A parent received information about an unrelated student because the families had the same last name.
- An employee accidentally included another student's name on a Section 504 consent form sent to parents.
- Students used an app that only required their name but voluntarily submitted their birthdates.[4]
- Students' first names and grade levels were left unredacted in the minutes from a Committee on Special Education meeting and were posted to the school's website.
- Records documenting student vaccination reports were thrown out in the trash and not shredded.
- A teacher had student PII (paper) in her purse, which was stolen.

Examples of student access being provided by teachers and/or school staff are:

- A teacher loaned her laptop to a student, who left their device at home. The student accessed the teacher's emails and viewed other students' PII.

[4] The Privacy Office had a meeting with the company, Sphero, which is reconfiguring its products so that students will not be able to submit their birthdates.

- 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.

Third-Party Contractors

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 infiltrated MOVEit with malware used to steal sensitive information. Private companies as well as federal, State and local governments were affected by the breach thereby affecting millions of individuals.
[7] The original Illuminate Education breach occurred in January 2022.

- 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.

Phishing

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.

Cyberattacks

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.

- Several educational agencies were made aware of cyberattacks through the New York State Division of Homeland Security and Emergency Services (DHSES) and immediately responded.

III. Disposition of Data Incident Report Filings

Education Law § 2-d and Section 121.10 of the regulations of the Commissioner of Education require educational agencies to report every discovery, or third-party contractor notification, of a breach or unauthorized disclosure of student, teacher, or principal data to the Chief Privacy Officer within 10 calendar days of discovery. When a data incident report is filed with the Privacy Office, there may be follow-up discussions with the educational agency to answer additional questions and, more importantly, to determine if PII was released and whether the proper procedures were implemented when a breach has occurred.

In 2023, several educational agencies improperly reported to the Privacy Office that they did not need to notify parents after suffering a data incident. Following discussions from the Privacy Office, however, these educational agencies agreed to notify parents and guardians. If a data incident report reveals a system compromise without evidence of unauthorized access of student, teacher or principal data, the Privacy Office will maintain contact with the educational agency or third-party contractor until a final determination is made as to whether there was unauthorized access to student, teacher or principal data. Additionally, after an investigation of a system compromise or breach, the Privacy Office may request that a Data Privacy/Cybersecurity Post-Incident Recovery Form be completed and submitted.

Collecting this data allows the Privacy Office to share information about system compromises and breaches within the education field to all of New York's educational agencies. This information can help identify where technical assistance may be necessary and assist education agencies in improving data privacy and security practices.

IV. Summary of Complaints 2023

Section 121.4 of the regulations of the Commissioner of Education and NYSED's § 2-d Bill of Rights for Data Privacy and Security authorize parents, eligible students, teachers, principals, and other staff of an educational agency to file complaints about possible breaches and unauthorized releases of PII. When a complaint is filed with NYSED's Privacy

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] Of the 16 additional complaints, 11 parents received a letter explaining why the Privacy Office was unable to render a determination. These decisions, summarized below, are available on the Privacy Office's webpage: Determinations of the Chief Privacy Officer | New York State Education Department.

1. Batavia City School District (issued 8/16/23):

A parent asserted that an employee of the school district inappropriately disclosed PII about a student to an emergency contact who was not the student's legal parent or guardian and was not authorized to receive such information. In the school district's response, it admitted that an employee spoke to the emergency contact regarding an incident after first being unable to contact the parent but added that no PII was shared with the emergency contact. Although a determination that the employee inappropriately disclosed PII could not be made, the Privacy Office encouraged the school district to review and update its policies, procedures and implementation regarding its annual data privacy and security awareness training.

2. Behavioral Strategies & Blue Sea Educational Consulting Inc. (issued 7/13/23):

Two school districts asserted that a former employee of Behavioral Strategies Licensed Behavior Analyst & LMSW PLLC inappropriately accessed students' data through a company account after leaving its employ. At the time of the alleged unauthorized access, the former employee was employed by a new, unrelated company. The Privacy Office did not find any evidence that the former employee was provided unauthorized access to

[8] Section 121.4 (c) of the Commissioner's regulations requires educational agencies to issue findings within 60 days of the filing of a complaint by a parent, eligible student, teacher, principal or other staff of an educational agency.

[9] An additional 16 complaints were reviewed or investigated by the Privacy Office but did not result in final determinations. One complaint filed in 2023 will be issued in 2024.

student data, or that any breach occurred. However, it was determined that the employee should have informed the former employer (Behavior Analyst & LMSW PLLC) of the identity of their new employer (Blue Sea Educational Consulting Inc.) and both companies should have ensured that the districts they serve were notified of the change in personnel. Both companies were required to submit evidence of updated guidance to the Privacy Office.

3. Bradford Central School District (issued 5/17/23):

An employee of the school district allegedly accessed a student's address to enable a former employee of the school to mail personal correspondence to the student's home. After an investigation by the school district, the employee admitted to the improper disclosure of the student's PII, the school district reviewed privacy expectations with the employee, and imposed disciplinary measures.

4. Brighton Central School District (issued 11/6/23):

A parent asserted that the school district improperly disclosed student PII, including health information, when it accidentally mailed the student's Section 504 individualized education plan to the incorrect household. After an investigation, the school district confirmed that a copy of the student's 504 education plan was accidentally mailed to the incorrect address. The school asserted that the unauthorized disclosure was limited to this student's PII; that it contacted the affected parties of the breach with a detailed explanation thereof; and that it mitigated any further unauthorized disclosure by ensuring the return of the copy accidentally sent to the incorrect household. The school district was ordered to file a data incident report with the Privacy Office within five days of the determination and was reminded of its obligation to address complaints or notifications of an improper release of student, teacher, or principal data.

5. Cairo-Durham Central School District (issued 12/1/23):

A parent complained that the school district posted a photograph of an entire class, which violated the complainant's request not to post photos of their child. The school district asserts that it's opt-out form was sent home with each student in the fall, which happened to be the same date that the photograph in question was posted to the school's Facebook page and website. The school district asserts that it never received an opt-out form from the student's parent. Because it remained unclear whether the parent submitted the

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.

7. Cold Spring Harbor Central School District (issued 8/4/23):

A parent alleged that a superintendent improperly responded to her email by including PII and copying members of the Board. The school district explained that the superintendent provided information about the student to address the parent's allegations and provide clarification to the Board. While the parent's concern regarding their child's PII being shared unnecessarily was valid, FERPA authorizes the sharing of educational records with school officials who have a legitimate educational interest in such information. Because the parties to the email had such an interest and there was no evidence that the Superintendent shared the student's information with the Board for improper or retaliatory reasons, the complaint was dismissed.

8. Elmira City School District (issued 8/24/23):

A parent asserted that the school district provided the parent's phone number to both the administrators and parents of students participating in the school district's My Brother's Keeper program, without consent. The school district admitted that it shared the address and cell phone information with the program's coordinator; that a group text was created using cell phone information inviting families to join the mentoring program; and that the student was removed from their distribution list upon learning that the parent wished to be

removed and the student would not participate in the program. The school district was encouraged to review and update its annual FERPA notification and directory information policies to ensure it only shares PII with school officials who have a legitimate educational interest in such information.

9. Grand Island Central School District (issued 3/17/23):

A parent complained regarding a text message received from a third-party vendor used by their child's school district, which contained an alert including the student's vaccination status, parent information, phone number, and the student's name. The school district responded that the text message was sent from the vendor that manages the school district's student management system, a subcontractor of Infinite Campus. The school district further indicated that it purchased the product from its BOCES. The BOCES provided copies of the contract with the vendor and the End User License Agreement as well as a link to the District's Data Privacy Inventory on its website. The BOCES asserted that it reviewed the contract and supporting documents to ensure that they met all regulatory requirements. After an investigation, the Privacy Office found that: (1) the vendor contract lacked a data security and privacy plan or the addendum required by Education Law § 2-d; (2) the supplemental information inaccurately identified the exclusive purpose for which PII was to be provided to the vendor; and (3) although the school district uploaded the supplemental information on its website, the information was difficult to find. The decision also held that the school district should have been able to explain the contractual arrangement to the parent upon request. For a remedy, the school district was directed to make its supplemental information more accessible to parents, ideally by placing the information on the same page as the Parents' Bill of Rights.

10. Dr. Richard Izquierdo Health & Science Charter School & Charter High School for Law and Social Justice (issued 3/28/23):

Complainant alleged that former staff members improperly retained PII before leaving their employment at the school to recruit students on behalf of their new employer. A representative for the former employees denied the allegations and asserted that families voluntarily reached out to the former staffers and provided the students' PII upon learning of their move to the new school. While the Privacy Office could not prove that any specific individual disclosed PII, the decision noted that the alleged actions, if proven, would constitute a violation of both FERPA and 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. Subsequently, the charter school has sought a review of the determination stating

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.

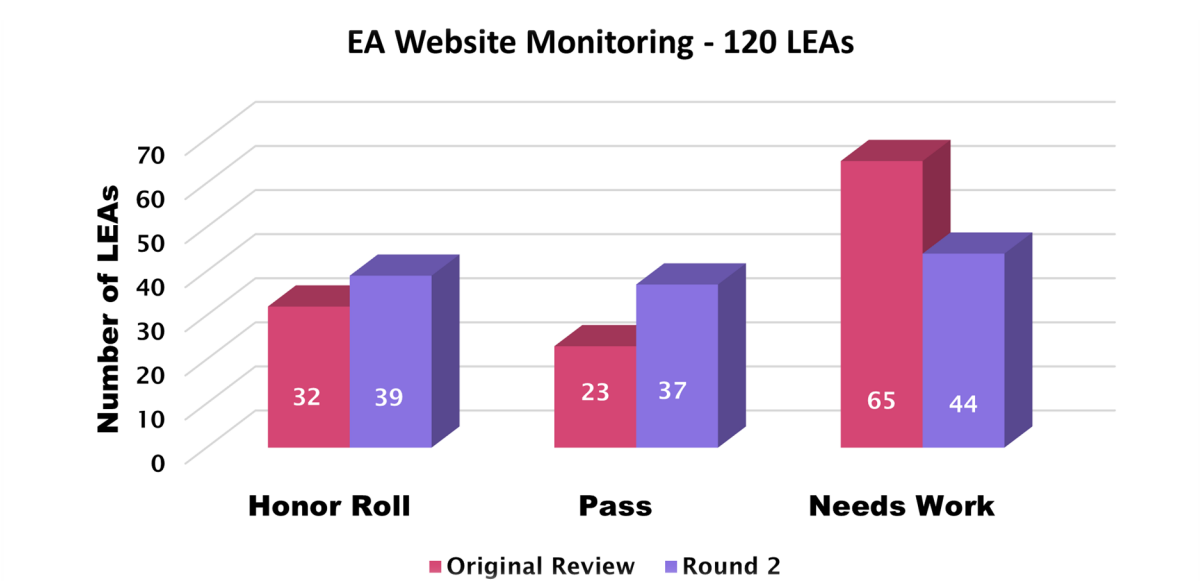
V. Monitoring of Educational Agencies' Web Sites

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

educational agencies received one of three types of designations, Honor Roll, Pass (minor issues) and Needs Work (larger issues). Any educational agency that did not meet the requirements of Education Law § 2-d and Part 121 received a Needs Work letter. Of the educational agencies that received a Needs Work letter, 56% of the School Districts and 100% of the Charter Schools responded by their due date. Those educational agency websites were evaluated again for a Round Two review. Once monitoring was complete, there were 39 honor roll educational agencies. The Privacy Office's January 2024 newsletter, shared with all educational agencies' data protection officers and superintendents, was devoted to the findings of the monitoring.



This report, previous annual reports, the Parents' Bill of Rights, information on how to file a complaint, information on student privacy and Education Law § 2-d, and the monitoring honor roll list can be found on NYSED's data privacy and security web page.