The University of the State of New York
Education Department

In the Matter of
Third-Party Contractor
Investigations of

Investigation and Determination by
New York State Education Dept.
Chief Privacy Officer

Behavioral Strategies Licensed
Behavior Analyst & LMSW LLC and
Blue Sea Educational Consulting Inc.

On April 28, 2023, the New York State Education Department's ("NYSED's") Chief Privacy Officer was made aware of a data incident involving a school district by the New York State Division of Homeland Security and Emergency Service's Cyber Incident Response Team. Thereafter, two school districts filed data incident reports with NYSED's Privacy Office indicating that a former employee (the "former employee") of Behavioral Strategies Licensed Behavior Analyst & LMSW PLLC ("Behavioral Strategies") inappropriately accessed student data through her Behavioral Strategies account after leaving the employ of that agency. At the time of the unauthorized access, the former employee was employed by an unrelated company, Blue Sea Educational Consulting Inc. ("Blue Sea"). NYSED's Privacy Office commenced an investigation into the matter.

Investigation:

By request, my office received statements from Behavioral Strategies and Blue Sea as well as an investigation report from counsel for the Riverhead Central School District ("Riverhead"). Riverhead's report included relevant emails between the former employee, another Blue Sea employee and Riverhead. According to this information, on March 31, 2023 the former employee left Behavioral Strategies and thereafter began employment at Blue Sea. The former employee did not inform her former employer, Behavioral Strategies where she would be working.

On April 17, 2023, a different Blue Sea employee emailed Riverhead, attempting to obtain access to Frontline (IEP Direct)[1] on behalf of the former employee so that the former employee could access information pertaining to three students with whom she was assigned to work. This email did not explain that the former employee was new to Blue Sea or that she formerly worked at Behavioral Strategies. Riverhead and Blue Sea employees continued to correspond from April 17 through 20, 2023. On April 20, a Blue Sea employee emailed Riverhead clarifying that "the Frontline account that was updated for [the former employee's] current clients and email was the account for her former agency supervisor [at Behavioral Strategies]. Is it possible to move that account back to [Behavioral Strategies] and maybe make a new one for [the former employee]?" A Riverhead administrator responded that she was unable to do so and that, instead, a new account needed to be made for Behavioral Strategies. The administrator further indicated that Behavioral Strategies would receive an email to set up a new log in/password. There is no indication that this information was shared with Behavioral Strategies.

On Friday, April 21, 2023, Behavioral Strategies "discovered that [its] Frontline account had been transferred to a different email address."[2] After contacting Riverhead, Behavioral Strategies learned that the former employee now works at Blue Sea. Because the Behavioral Strategies Frontline account was mistakenly and temporarily transferred to the former employee, the account was considered "compromised."

Were this not convoluted enough, an administrator at yet another school district, the Miller Place School District ("Middle Place"), entered the fray. At the request of Behavioral Strategies, Miller Place reset its Frontline account with the company's email address. However, Miller Place incorrectly believed that the problem arose because it was the practice of the executive director of Behavioral Strategies to share her Frontline account credentials with all employees, rather than create individual accounts for each employee.[3] Based on this false supposition, Miller Place shared the information with Eastern Suffolk (ES) BOCES, who proceeded to notify ten school districts that Behavioral Strategies' Frontline account was compromised and that its executive director shared her Frontline account credentials with her employees. This led to data incident reports being filed with my office, even though no school reported evidence that students' records were viewed or otherwise accessed by either Behavioral Strategies or the former employee between April 17 and 21, 2023.

---

[1] Frontline (IEP Direct) is a web-based computer software system designed to draft, revise, and distribute Individualized Education Programs ("IEPs") for special education students and Section 504 Accommodation Plans.

[2] The account was transferred to an email address of the former employee at riverhead.net.

[3] Rather than have Frontline accounts for each employee, Behavioral Strategies states that they maintain one Frontline account and the "the Company transfers ... relevant student records (including, typically IEPs) into each employee's ReThink BH account."

Findings:

There is no evidence that the former employee was provided unauthorized access to student data. What occurred here was a failure—or, more accurately, an unwillingness—to communicate. A phone call or two could have clarified many of the misunderstandings that occurred when Blue Sea sought to establish a Frontline account with Riverhead for the former employee. Instead, the misunderstandings compounded to an almost farcical level involving two businesses, ten school districts a BOCES, and my office.

Even if an employee leaves an employer on less than cordial terms, it behooves both employer and employee to share information as necessary and communicate in a professional manner. In this case, Behavioral Strategies and Blue Sea serve many of the same school districts. As such, the former employee should have informed Behavioral Strategies of the identity of her new employer and both companies should have ensured that the districts they serve were properly notified of the change in personnel.

Determination

Behavioral Strategies and Blue Sea must submit evidence to my office, by September 15, 2023, that:

1) All of their employees received data privacy and security training. Evidence will consist of a list of names and dates that the training occurred.
2) They have implemented internal policies to inform the school districts they serve of any personnel changes that include employees who work directly with students. Evidence will consist of a copy of the policy and its effective date.

July13, 2023
Louise DeCandia
Chief Privacy Officer
NYSED