CLIENT NEWS BRIEF

Feds Offer Guidance on Recent School Data System Hacks

October 2017
Number 69

An arm of the U.S. Department of Education is warning schools and colleges to prepare themselves to address a new threat from cyber criminals hacking into schools' data systems.

On October 16, 2017, the Department's Federal Student Aid office (FSA) warned that cyber criminals attempted to extort money from school districts in Texas, Montana and Iowa by threatening to publicly release sensitive student information. According to news reports, the hacker or hackers, going by the moniker "The Dark Overlord," sent messages directly to students or parents threatening to harm or kill children, prompting closures in two of the three school districts that have admitted to being targeted so far.

Law enforcement officials have said that the threats of violence are not credible, adding that the suspect is overseas. Still, the threats and the hacker's release of data online and with media outlets, including voicemail messages from some of the victims, mark an escalation in cyber criminals' tactics. School districts across the country, including in California, have been grappling with ransomware attacks in which hackers infiltrate schools' computer systems, render data inaccessible and then threaten to destroy the data unless a ransom is paid. (See 2017 TIP Jar #1.)

According to the advisory, FSA believes that the hackers are targeting school districts with weak data security or well-known vulnerabilities that enable them to access sensitive data. It adds that the attacks could come in the form of direct electronic attacks on computers or applications, malicious software or email "phishing" attacks that enable hackers to access sensitive systems through individual employees.

FSA is advising schools and colleges to protect their organizations by encouraging educational institutions to:

- Conduct security audits to identify weaknesses and update or patch vulnerable systems;
- Ensure proper audit logs are created and reviewed routinely for suspicious activity;
- Train staff and students on data security best practices and phishing and social engineering awareness; and
- Review all sensitive data to verify that outside access is appropriately limited.

The advisory recommends that schools or colleges affected by such an attack contact local law enforcement immediately. It also requests that affected K-12 schools email privacyTA@ed.gov so that the spread of any threats may be monitored.

The advisory also reminds colleges that they are required to notify the Office of Federal Student Aid via email regarding any data breaches.

Manuel F. Martinez
Partner
Walnut Creek Office
mmartinez@lozanosmith.com

Penelope R. Glover
Senior Counsel and Chair
Technology & Innovation Practice Group
Walnut Creek Office
pglover@lozanosmith.com

Lozano Smith
ATTORNEYS AT LAW

Additional resources for avoiding, responding to and recovering from cyberattacks include the Privacy Technical Assistance Center website and the Federal Student Aid office's cybersecurity web page.

Separate and aside from the guidance, both federal and state law protect the privacy of student information, and state law requires public agencies to report data breaches to affected parties. In 2016, state lawmakers enacted a bill prohibiting schools from collecting students' Social Security numbers in an effort to protect students from identity theft. (See 2017 Client News Brief No. 13.)

Lozano Smith has been at the forefront of addressing cyber security issues, and will be further addressing these issues in upcoming editions of the TIP Jar. To subscribe to the TIP Jar or to download our latest issue, click here.

For more information regarding these new cyberattacks or on a public agency's obligation to secure student and employee information, please contact the authors of this Client News Brief or an attorney in our Technology and Innovation Practice Group or at one of our eight offices located statewide. You can also visit our website, follow us on Facebook or Twitter or download our Client News Brief App.