


Hackers escalate: leak 200k CCSD students' data; claim to still have access to CCSD email system

 databreaches.net/hackers-escalate-leak-200k-ccsd-students-data-claim-to-still-have-access-to-ccsd-email-system/

Dissent

October 27, 2023

Clark County School District (CCSD) in Nevada informed parents and employees that they became aware of a “cybersecurity incident” on October 5. Three weeks later, the district had not fully recovered from the attack and parents were complaining about the district’s lack of transparency about what was stolen in the breach. Disturbingly, while the district has not disclosed the scope of the breach of student information, the hackers started disclosing it this week – and in the worst way possible — by leaking 200,000 students’ information and numerous other files with personal information. There may be more to come.

Yesterday, Tiffany Lane of [News3LV](#) and Julie Wooten of [Las Vegas Review-Journal](#) reported that parents were increasingly concerned about the breach after receiving emails purportedly from the hackers with their children’s personal information. One parent described the email they received as, “Warning me that my children’s information was released or hacked into and it had three PDF files. Each one had my children’s picture, all of their contact information, email addresses, student ID numbers, my information, our address.”

That mother was right to be concerned and to think it was related to the breach. Files with those data elements had been stolen and some were leaked this week. As DataBreaches reported yesterday, a number of files that appeared to be from the district were leaked on a file-sharing site earlier this week. The post with the links to the files was removed (probably by the filehost), but DataBreaches described the contents of some of the leaked files and provided [screenshots and a list of the archive names](#).

In response to that post, DataBreaches was contacted by an individual claiming to be from the hackers. They introduced themselves as “SingularityMD.” DataBreaches notes that the name “SingularityMD” has no obvious connection to the website with the same domain name that automates physician note-talking with AI. The email address used was an email address from the Coalinga-Huron Unified School District that the hackers immediately indicated was not theirs and would not reach them.

The Hackers Tell Their Side

“SingularityMD” provided this site with a link to a second leak post on a file-sharing site. That post, dated October 25, contained a statement as well as links to yet more files. The statement was intriguing on a number of levels, in part because it suggested some detailed

knowledge of the district's security policies and past practices. [Note: DataBreaches does not know if SingularityMD is really one person or more than one, but will use the plural form.]

Their statement began:

We SingularityMD (the hack team), would like to make a statement for clarification.

CCSD did not detect a security issue, we emailed them to tell them we had been in their network for a few months.

For 6 years they forced students to use their birthday as their password, resetting the passwords back to their birth date each year, they even prevented the students from securing their accounts.

The statement then made clear that there was an extortion demand:

We asked for less than one third of the Jesus F Jara's annual salary in exchange for destroying the stolen data.

The callousness and incompetence of the leadership at CCSD is astounding, not only did they not cooperate, it is clear they did not communicate with principals and have still not plugged their leaky ship, meaning we still have access to the network.

Superintendent Jara's annual salary is \$395,000.00 per year. As in a previous extortion demand incident in 2020, the district reportedly did not agree to pay. The attackers probably should not have been surprised in light of the district's past behavior.

But of note, the threat actors claimed that they still have access to the district's network. That last claim received support last night when an email arrived for DataBreaches that appeared to be from a named student at CCSD. The From: line had the format: FIRSTNAME Lastname [STUDENT] <[email_protected]>. A check of the Master Register file leaked by the group indicated that a student by that name is enrolled at the George E. Harris Elementary School. A check of the header for the email returned: X-Spam-Status: No, score=-0.1 required=.6 tests=DKIM_SIGNED, DKIM_VALID, DKIM_VALID_AU, HTML_MESSAGE, RCVD_IN_DNSWL_NONE, RCVD_IN_MSPIKE_H3, RCVD_IN_MSPIKE_WL. So **it appears that the hackers still have access to the district's email server**. The extent of their access to other parts of the network is unknown to DataBreaches, and the hackers did not provide this site with a way to contact them with questions. In any event, their post of October 25 continued:

We are not short sighted, and so we kept our end of the bargain. After all we are already working on data collection for two other organizations. Should we have received payment, the data would be destroyed and we hope to demonstrate that with the next organization who pays.

The statement then repeated what was evident from their first leak: that they do have personal information on students. This time, though, they started leaking more student information:

As promised to them in our initial correspondence we are now leaking the 200k student profiles we extracted from their network yesterday, these profiles include a photo, birth date, person ID, student Number, State Student ID, Email, Language, Race / Ethnicity, Household names, relationships and contact information, outside household contact information.

One final tip for CCSD, we will continue to cause trouble until you pay, or you finally kick us out of your network.

A list of twelve zipped archives, by grade, with links to the zipped archives followed the statement. There was also a Master Register, containing “A list of all 300k+ students, birthdate, grade.” All of the zipped archives were on a clearnet file-sharing site. And because the earlier leak post had been removed, the October 25 leak also reposted the earlier leak’s links to clearnet and deep web sites.

Once again, DataBreaches reached out to CCSD via their web site contact to ask for a statement about the leak of personal information of students. DataBreaches also asked the district whether it was true that the attackers still had access on October 24, the day they claimed to have exfiltrated the data on 200k students. Note: that inquiry was sent earlier in the day before DataBreaches received an email demonstrating that the hackers still have access to the email server.

Once again, no reply was received from the district. Other news outlets report similar outcomes: the district is not responding to specific questions from the media seeking the kinds of information parents and employees want to know.

Yesterday, DataBreaches reported student personal information in the first leak included attendance records, incident reports, and some medically related information. There were also other files in that first leak. In contrast, the second leak was specific to student demographic information, as described in their statement. The following is a screenshot of a “Person Summary Report” that has been redacted by DataBreaches. It is one of 14,804 such pdf files in the leaked “1st Grade CCSD” archive. The data elements in the report contain the student’s name, their student ID, their date of birth, their person ID, their student email address, their picture, and household members’ information including parents’ and siblings names, cellphone numbers, email addresses, and other contact information. Race and ethnicity information is also included and other fields permit reporting of non-household relationships:

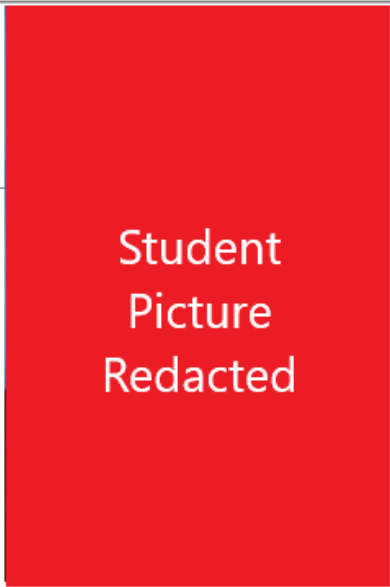
Person Summary Report

Person ID: [REDACTED]

Birth Date: [REDACTED]
Staff Number: [REDACTED]
Person GUID: [REDACTED]
Student Number: [REDACTED]
Student State ID: [REDACTED]
Staff State ID: [REDACTED]

Contact Information:

Other Phone: [REDACTED]
Work Phone: [REDACTED]
Cell Phone: [REDACTED]
Pager: [REDACTED]
Email: [REDACTED]
Secondary Email: [REDACTED]
Preferred Language: en_US



Primary Household: [REDACTED]

Household Phone: [REDACTED]

Address(es): [REDACTED]

[REDACTED]	Mother	Cell: [REDACTED] Email: [REDACTED]
[REDACTED]	Father	Cell: [REDACTED] Other: [REDACTED] Email: [REDACTED]
[REDACTED]	Sibling	Email: [REDACTED]

Non-Household Relationships

Race/Ethnicity Information

State Race/Ethnicity: [REDACTED]
Federal Race/Ethnicity Designation: [REDACTED]
Race(s): [REDACTED]
Hispanic/Latino: [REDACTED]
Race/Ethnicity Determination: [REDACTED]
Date Entered US: [REDACTED]
Date Entered US School: [REDACTED]

Person Comments: [REDACTED]

Contact Information Comments: [REDACTED]

Image: DataBreaches.net

In addition to the individual grade archives, there was also the Master Register file in the newer leak. The Master Register file has 331,265 rows, one for each student. The Master Register .csv file contained students' first, middle, and last names, their date of birth, their school and grade, their race and ethnicity, as well as their start date and end date.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	SchoolName	StateID	LastName	FirstName	MiddleNar	Birthdate	Gender	RaceEthnic	StartDate	StartStatus	EndDate	EndStatus	Grade	Track	SchoolCode
2	NW Career-Technical Academy ES								8/7/2023						075
3	NW Career-Technical Academy ES								8/7/2023						075
4	NW Career-Technical Academy ES								8/7/2023						075
5	NW Career-Technical Academy ES								8/7/2023						075
6	NW Career-Technical Academy ES								8/7/2023						075
7	NW Career-Technical Academy ES								8/7/2023						075
8	NW Career-Technical Academy ES								8/7/2023						075
9	NW Career-Technical Academy ES								8/7/2023						075
10	NW Career-Technical Academy ES								8/7/2023						075
11	NW Career-Technical Academy ES								8/7/2023						075
12	NW Career-Technical Academy ES								8/7/2023						075
13	NW Career-Technical Academy ES								8/7/2023						075
14	NW Career-Technical Academy ES								8/7/2023						075
15	NW Career-Technical Academy ES								8/7/2023						075
16	NW Career-Technical Academy ES								8/8/2023						075
17	NW Career-Technical Academy ES								8/7/2023						075
18	NW Career-Technical Academy ES								8/7/2023						075
19	Reedom, Carolyn S ES								8/7/2023						084
20	Reedom, Carolyn S ES								8/7/2023						084
21	Reedom, Carolyn S ES								10/16/2023						084
22	Reedom, Carolyn S ES								8/7/2023						084
23	Reedom, Carolyn S ES								8/7/2023						084
24	Reedom, Carolyn S ES								8/7/2023						084
25	Reedom, Carolyn S ES								8/7/2023						084
26	Reedom, Carolyn S ES								8/7/2023						084
27	Reedom, Carolyn S ES								8/7/2023						084
28	Reedom, Carolyn S ES								8/7/2023						084
29	Reedom, Carolyn S ES								8/7/2023						084

The Master Register .csv file contained students' first, middle, and last names, their date of birth, their school and grade, their race and ethnicity, as well as their start date and end date. Image and redaction: DataBreaches.net

Lessons Learned?

CCSD is the fifth largest school district in the nation, and this is not their first cyberattack (they suffered a ransomware attack three years ago). What did they do after the first one to harden their security? Looking at their budget for the past few years, there has been only one entry specifically described as "Service, Cyber Security." Mosaic451 LLC had contracts for the 2021-2022 and 2022-2023 school years for \$930,300 and then \$931,000. For the 2023-2024 year, however, the district's proposed expenditure for them was \$369,813. No other service was listed in the budget summary specifically for "cybersecurity." Did the district decide it no longer needed some services, or did it have an alternative plan or providers to address them, or is there some other explanation? When was the district's last risk assessment and what did it do in response to it? Will the hackers tell us how they gained access if the district doesn't? And what lessons did the district learn about communications and transparency from the 2020 incident?

Transparency is Crucial

On October 16, Fox5 cited a statement by the district that disclosed that their investigation to that point had found that the attacker had accessed a "limited amount of personal information." They did not define "limited."

When parents and students expressed concerns, did the district reveal more about what it knew so far? The district gave them a nonspecific statement that it was still working to determine the scope and people who were affected would get letters about how to protect

themselves.

“Rest assured that we are committed to sharing information as it becomes available,” CCSD said. Then why didn’t it share that it knew student data had started being leaked this week? “Cooperating with the FBI” is not a reason to not disclose unless the FBI has specifically requested you not disclose, and in that case, entities always report that they have been asked to delay or withhold notification so as not to interfere with an investigation. CCSD has not claimed that they have been asked not to disclose by the FBI, so reference to the FBI is irrelevant to their failure to disclose. How long would it take for the district to review the first leak and recognize whether those files did come from their system or not?

The district states that those with questions can call a dedicated assistance line at 888-566-5512 between 6:00 a.m. and 6:00 p.m., Monday through Friday, excluding holidays. Will 200,000 parents now start calling them? And will callers be able to get through if there is a flood of calls?

School districts tend to be soft targets for hackers. But decisions about transparency affect trust between the district and the community and at this point, it would be understandable if taxpayers, parents, and some employees want heads to roll for keeping them in the dark. But who should be held accountable for the breach and who should be held accountable for the lack of transparency? By accountability, DataBreaches does not mean throwing an underpaid and overworked IT employee under the bus.

Victims of a breach — students, their parents, and employees — should not be first finding out from criminals that their personal information has been stolen and leaked publicly. They should be finding out first from the entity that was responsible for securing their data.

A Note to SingularityMD

Please provide a way to contact you to ask questions. Email, Telegram, Jabber, Tox, Signal.... take your pick and let me know. Thanks.

Update: they gave me a way to contact them.

Related Posts:

- [Has private financial information been exposed in...](#)
- [NV: Personal information accessed in Clark County...](#)
- [NV: Clark County School District notifies parents...](#)
- [NV: CCSD magnet school website experiences data loss](#)
- [NV: CCSD says data breach has exposed student, staff...](#)