Elmbrook Students, Families and Staff Members,

Last week, we reported to you that on August 23, 2022, our District detected unauthorized access to a limited portion of our network by an individual(s). As our technology team worked to secure our network, we immediately commenced a prompt and thorough investigation with several expert resources, including external cybersecurity professionals experienced in handling these types of incidents. During this investigation, we have learned that a limited amount of Elmbrook data was posted on the dark web. While typically this criminal activity is used to extort money from the victim organization, in our case no such ransom was requested and the District never engaged with this external threat actor.

Based on the information available right now, the posted data of note is primarily the personal information of employees of the District and, in some cases, their dependents. While we have no evidence that any staff information has been misused, we have initiated several actions to protect staff from the potential misuse of your information. This includes offering impacted staff a complimentary, one-year membership of Experian IdentityWorks Credit Monitoring along with a hotline number for support questions related to this data exfiltration. Impacted employees will receive more information about these details next week in a letter mailed to your home address.

Additionally, the District has also identified a limited amount of student educational records that were posted to the dark web. This data **does not** include Social Security numbers (the District does not collect these) and **at no time** was access to our Infinite Campus Student Information System compromised. The District is working to directly notify this small number of current and former students and their families in accordance with state and/or federal law.

I apologize for any inconvenience or concern this incident may cause you. Unfortunately, cyber criminals continue to victimize individuals and organizations worldwide on a daily basis. In fact, the organization responsible for posting the District's data to the dark web was highlighted on Monday in a ransomware warning to K-12 school districts by the Federal Bureau of Investigation (FBI) and was associated with a cyber attack on the Los Angeles Public Schools over the weekend.

I am grateful for the resiliency of our 9,000 staff and students who responded to last week's password change with grace and understanding. Our entire leadership team takes this matter very seriously and we will continue to work with local and national resources, as well as appropriate federal agencies, to take significant measures to protect the information entrusted to us.

Dr. Mark Hansen, Superintendent
School District of Elmbrook