CCSD
CLARK COUNTY
SCHOOL DISTRICT

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

The Clark County School District ("CCSD") writes to inform you of a recent incident that may affect the security of your information. The confidentiality, privacy, and security of information in CCSD's care is one of its highest priorities and CCSD takes this incident very seriously. Although CCSD has not received any reports of actual or attempted misuse of the impacted information, CCSD is providing this notice in an abundance of caution.

What Happened? On the morning of August 27, 2020, certain CCSD systems became infected with a virus that prohibited access to certain files. Upon discovery, CCSD immediately notified law enforcement and began an investigation, which included working with third-party forensic investigators, to determine the full nature and scope of the incident and to secure the CCSD network. While the investigation into the full scope of this incident is ongoing, the investigation determined that CCSD was the victim of a criminal ransomware attack.CCSD's investigation further determined CCSD systems were subject to unauthorized access on or about August 25, 2020. As a result, certain current and former employee information may have been accessed or acquired by the unauthorized actor.

What Information Was Involved? While the investigation was able to determine that certain CCSD systems were accessed, the investigation is still working to determine whether your specific sensitive information was actually accessed or acquired by the unauthorized actor. However, on or about September 25, 2020, CCSD's investigation determined that certain current and former employee information was impacted by this incident and available to the unauthorized actor. Therefore, **in an abundance of caution**, CCSD is notifying you of this incident because your name, date of birth, address, and/or Social Security number **may** have been present in the affected systems at the time of the incident.

What Are We Doing? Currently, CCSD is working diligently to determine the full nature and scope of this incident and is cooperating with law enforcement's investigation. Upon discovering this incident, CCSD immediately launched an investigation, took steps to secure CCSD systems, and began a review to determine what personal data was at risk. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures, to implement additional safeguards, and to provide additional training to employees on data privacy and security. We will also be notifying state and federal regulators, as required.

As an added precaution, we are also offering you complimentary access to twelve (12) months of credit monitoring and identity theft restoration services through TransUnion. We encourage you to activate these services, as we are not able to act on your behalf to activate them for you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What Can You Do. We encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information* for additional steps you may take and information on what you can do to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. You may also activate the complimentary credit and identity monitoring services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions about this incident, please call CCSD's dedicated assistance line at 888-490-0594, Monday through Friday between the hours of 6:00 a.m. to 6:00 p.m., Pacific Time. You may also write to CCSD at 4828 S. Pearl Street, Las Vegas, NV 89121 or visit our website at www.ccsd.net.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Clark County School District

Steps You Can Take to Help Protect Your Information

Enroll in Credit and Identity Monitoring

Complimentary One-Year *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. Mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Ave. NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov.

EXHIBIT B

NOTICE OF DATA PRIVACY INCIDENT

The Clark County School District ("CCSD") is providing notice of a recent incident that may affect the security of information pertaining to individuals, including certain current and former employees. The confidentiality, privacy, and security of information in CCSD's care is one of its highest priorities and CCSD takes this incident very seriously. Although CCSD has not received any reports of actual or attempted misuse of the impacted information, CCSD is providing this notice in an abundance of caution.

What Happened? On the morning of August 27, 2020, certain CCSD systems became infected with a virus that prohibited access to certain files. Upon discovery, CCSD immediately notified law enforcement and began an investigation, which included working with third-party forensic investigators, to determine the full nature and scope of the incident and to secure the CCSD network. While the investigation into this incident is ongoing, it was determined that CCSD was the victim of a criminal ransomware attack and is working to restore all systems to secure, full functionality.

What Information Was Involved? While CCSD's investigation is ongoing and has been unable to determine whether any specific file containing sensitive information was actually accessed or acquired by the unauthorized actor, CCSD's investigation determined that certain current and former employee information may have been accessed or acquired by the unauthorized actor. Therefore, in an abundance of caution, CCSD is notifying individuals, including certain current and former employees, of this incident whose name and Social Security numbers were present in the affected systems at the time of the incident.

What Are We Doing? Currently, CCSD is working diligently to determine the full nature and scope of this incident and is cooperating with law enforcement's investigation. Upon discovering this incident, CCSD immediately launched an investigation and took steps to secure its systems and determine what personal data was at risk. As part of CCSD's ongoing commitment to the security of information in its care, CCSD will be reviewing existing policies and procedures and implementing additional safeguards. CCSD will also be individually notifying affected individuals as well as state and federal regulators, as required.

For More Information. You may have questions about this incident that are not addressed in this letter. If you have additional questions and are impacted by this incident, please call CCSD's dedicated assistance line at 888-490-0594 between the hours of 6:00am to 6:00pm Pacific Time. You may also write to CCSD at 4828 S. Pearl Street, Las Vegas NV 89121.

What Can You Do. CCSD sincerely regrets any inconvenience this incident may have caused. CCSD encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.