EXHIBIT A

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>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Lodi Unified School District (the "District") writes to notify you of a recent incident that may impact the privacy of certain information provided to us. You may have received a similar letter in the mail on or about November 5, 2021. Please note that this is not notice of a second incident; this is a follow up communication to ensure all potentially impacted individuals are notified. We take this incident very seriously and are providing you information about the incident, our response, and steps you can take to help protect your information including complimentary credit monitoring services that we are offering you.

What Happened? On or about October 3, 2021, we experienced a network disruption that impacted our ability to access certain District files and systems. We immediately began an investigation, which included working with third-party specialists to determine the full nature and scope of the activity. Our investigation is ongoing; however, it was able to determine that certain segments of our network were accessed during the incident. Therefore, in an abundance of caution, we conducted a review of the contents of the potentially impacted network locations to determine the type of information contained therein and to whom the information related. On October 13, 2021, we determined that files containing certain current and former employee information was present in the potentially impacted network locations. To date, the investigation has not revealed any evidence of actual or attempted misuse of your information as a result of this incident. On January 10, 2022, we discovered additional contact information for a limited group of people. We are therefore sending follow up communications to that limited group in order to ensure all potentially impacted individuals are made aware of this incident.

What Information Was Involved? The investigation revealed that the information potentially impacted included your first and last name as well as your Social Security number, and may have also included your medical information.

What We Are Doing. In response to this incident, we changed account passwords and enhanced security protocols. We are working with third party specialists to harden our network and are reviewing our policies and procedures related to data protection. Our investigation into this incident remains ongoing.

What You Can Do. As previously stated, to date, we have no evidence of actual or attempted misuse of your information as a result of this incident. However, in an abundance of caution, we are providing you access to <<12/24>> months of credit monitoring and identity protection services through Equifax at no cost to you. If you received a previous letter and have already enrolled in the credit monitoring, there is nothing additional you need to do. However, if you did not receive a previous letter or have not yet enrolled, instructions about how to enroll in these services and additional resources available to you are included in the enclosed *Steps You Can Take to Protect Your Information.*

For More Information. We understand you may have questions about this incident that are not addressed in this letter. You may contact our dedicated assistance line at 855-675-3119, Monday through Friday from 6 am – 6 pm PST (excluding major U.S. holidays), or write to us at 1305 E. Vine Street, Lodi, CA 95240.

We sincerely regret any concern this incident may cause you. The privacy and security of information is important to us, and we will continue to take steps to protect information in our care.

Sincerely,

Leonard Kahn, Chief Business Officer
Lodi Unified School District

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring / Identity Protection

Enrollment Instructions

Go to ***www.equifax.com/activate*** and enter your unique Activation Code of <<*ACTIVATION CODE*>> then click "Submit" and follow these 4 steps:

1. **Register:** Complete the form with your contact information and click "Continue". If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:** Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment. Click "View My Product" to access the product features.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications when your personal information, such as Social Security number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft (conditions apply).

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit 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 credit freeze 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. 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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

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>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Lodi Unified School District (the "District") writes to notify you of a recent incident that may impact the privacy of certain information provided to us. We take this incident very seriously and are providing you information about the incident, our response, and steps you can take to help protect your information including complimentary credit monitoring services that we are offering you.

What Happened? On or about October 3, 2021, we experienced a network disruption that impacted our ability to access certain District files and systems. We immediately began an investigation, which included working with third-party specialists to determine the full nature and scope of the activity. Our investigation is ongoing; however, it was able to determine that certain segments of our network were accessed during the incident. Therefore, in an abundance of caution, we conducted a review of the contents of the potentially impacted network locations to determine the type of information contained therein and to whom the information related. On December 10, 2021, we determined that files containing certain parent and district volunteer information was present in the potentially impacted network locations. To date, the investigation has not revealed any evidence of actual or attempted misuse of your information as a result of this incident.

What Information Was Involved? The investigation revealed that the information potentially impacted included your first and last name as well as your Social Security number.

What We Are Doing. In response to this incident, we changed account passwords and enhanced security protocols. We are working with third party specialists to harden our network and are reviewing our policies and procedures related to data protection. Our investigation into this incident remains ongoing.

What You Can Do. As previously stated, to date, we have no evidence of actual or attempted misuse of your information as a result of this incident. However, in an abundance of caution, we are providing you access to <<12/24>> months of credit monitoring and identity protection services through Equifax at no cost to you. Instructions about how to enroll in these services and additional resources available to you are included in the enclosed *Steps You Can Take to Protect Your Information.*

For More Information. We understand you may have questions about this incident that are not addressed in this letter. You may contact our dedicated assistance line at 855-675-3119, Monday through Friday from 6 am- 6 pm PST (excluding major U.S. holidays), or write to us at 1305 E. Vine Street, Lodi, CA 95240.

We sincerely regret any concern this incident may cause you. The privacy and security of information is important to us, and we will continue to take steps to protect information in our care.

Sincerely,

Leonard Kahn, Chief Business Officer
Lodi Unified School District

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring / Identity Protection

Enrollment Instructions

Go to ***www.equifax.com/activate*** and enter your unique Activation Code of *<<ACTIVATION CODE>>* then click "Submit" and follow these 4 steps:

1. **Register:** Complete the form with your contact information and click "Continue". If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:** Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**: Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment. Click "View My Product" to access the product features.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft (conditions apply).

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit 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 credit freeze 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. 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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

EXHIBIT B

Notice of Data Incident
January 14, 2022

Lodi, CA – Lodi Unified School District ("the District") has become aware of a data incident that may have impacted individuals' information.

On October 3, 2021, the District experienced a network disruption that impacted its ability to access certain District files and systems. The District immediately began an investigation, which included working with third-party specialists to determine the full nature and scope of the activity. The District's investigation was able to determine that certain segments of the District's network were accessed during the incident. Therefore, in an abundance of caution, the District conducted a review of the contents of the potentially impacted network locations to determine the type of information contained therein and to whom the information related.

On October 13, 2021, the investigation confirmed that a limited amount of information may have been accessed during this incident. Therefore, the District immediately undertook a thorough review of its systems to identify potentially affected individuals and any information that may have been at-risk as a result of the incident. Although there is no evidence to suggest actual or attempted misuse of information as a result of this incident, on November 5, 2021, the District provided written notification to current and former staff members with sensitive information contained within the network. Our investigation continued and identified other discrete populations of individuals with sensitive information potentially impacted. Those individuals were also provided with written notification.

The types of information that could be potentially impacted varies by individual but includes name and one or more of the following data elements: Social Security number, driver's license number, CA identification card number, tax identification number, passport number, military identification number, or other unique identification number used on a government document, account number or credit or debit card number, medical information, or username or email address in combination with a password or security question and answer that would permit access to an online account. **Please note that student Social Security numbers were not impacted by this incident.**

In response to this incident, the District changed account passwords and is implementing additional security measures. In an abundance of caution, the District is offering potentially impacted individuals access to credit monitoring and identity protection services.

To obtain more information about this incident, please contact the District's dedicated assistance line at 855-675-3119, Monday through Friday (except U.S. holidays), from 6 am- 6 pm PST. Individuals may also write to the District at 1305 E. Vine Street Lodi, CA 95240.

Individuals are encouraged to remain vigilant against incidents of identity theft and fraud by reviewing credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors.

In addition, the District has notified the FBI and any applicable state regulators of this incident.

Lodi Unified School District deeply regrets any inconvenience or concern this incident may cause. Please contact the call with questions.

Media Contact: Chelsea Vongehr, Public Information Officer
Name: Chelsea Vongehr, Public Information Officer
Email / Phone number: (209) 331-8043 cvongehr@lodiusd.net

Lodi Unified School District Provides Notice of Data Security Incident
January 14, 2022

On October 3, 2021, Lodi Unified School District ("the District") experienced a network disruption that impacted our ability to access certain District files and systems. The investigation included working with third-party specialists to determine the full nature and scope of the activity. The District's investigation was able to determine that certain segments of the District's network were accessed during the incident. Therefore, in an abundance of caution, we conducted a review of the contents of the potentially impacted network locations to determine the type of information contained therein and to whom the information related.

On October 13, 2021, the investigation confirmed that a limited amount of information may have been accessed during this incident. Therefore, we immediately undertook a thorough review of District systems to identify potentially affected individuals and any information that may have been at-risk as a result of the incident. Although there is no evidence to suggest actual or attempted misuse of information as a result of this incident, on November 5, 2021, we provided written notification to current and former staff members with sensitive information contained within the network. Our investigation continued and identified other discrete populations of individuals with sensitive information potentially impacted. Those individuals were also provided with written notification.

The types of information that could be potentially impacted varies by individual but includes first and last name and one or more of the following data elements: Social Security number, driver's license number, CA identification card number, tax identification number, passport number, military identification number, or other unique identification number used on a government document, account number or credit or debit card number, medical information, or username or email address in combination with a password or security question and answer that would permit access to an online account. **Please note that student Social Security numbers were not impacted by this incident.**

In response to this incident, we changed account passwords and are implementing additional security measures. To obtain more information about this incident, individuals should contact the District's dedicated assistance line at 855-675-3119, Monday through Friday (except U.S. holidays), from 6 am- 6 pm PST. Individuals may also write to the District at 1305 E. Vine Street Lodi, CA 95240.

In general, we encourage potentially impacted individuals to remain vigilant against incidents of identity theft and fraud by reviewing credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228.

Individuals have the right to place an initial or extended "fraud alert" on a credit file at no cost. If individuals are a victim of identity theft, they are entitled to an extended fraud alert lasting seven years. As an alternative to a fraud alert, they have the right to place a "credit freeze" on a credit report. The credit freeze is designed to prevent credit, loans, and services from being approved without consent. Pursuant to federal law, individuals cannot be charged to place or lift a credit freeze on your credit report.

Should individuals wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion	**Experian**	**Equifax**
1-800-680-7289	1-888-397-3742	1-888-298-0045
transunion.com	experian.com	equifax.com
P.O. Box 2000	P.O. Box 9554	P.O. Box 105069
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348

Individuals can further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps to protect their personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or their state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC.