

23240



North East Educational and Developmental Support Center

September 30, 2021

<<first>> <<last>>  
<<street>>  
<<city>>, <<state>> <<zip>>

**IMPORTANT INFORMATION – PLEASE REVIEW CAREFULLY  
NOTICE OF DATA SECURITY INCIDENT**

Dear <<first>> <<last>>:

I am writing to tell you about a recent data security incident at North East Educational and Developmental Support Center (“NEEDS”) that may have resulted in unauthorized access to information that we maintain about our current or former employees, their relatives, clients who we treat or other persons associated with NEEDS. **At this time, we have no indication that any of your personal information has been inappropriately used by anyone.** We are providing this notice as a precautionary measure, to inform you of the incident, explain the complimentary services we are offering you, and suggest ways that you can help protect your information.

**What Happened**

On July 5, 2021, we learned that a NEEDS’ employee email account had been used in a targeted attempt to complete an unauthorized wire transfer of NEEDS’ money. We successfully detected and responded to the attempt before any payments were redirected. We also worked with cyber security experts so that we could better understand what happened and, more importantly, prevent something like this from happening again.

**What Information Was Involved**

On August 2, 2021, we first discovered that the impacted email account contained protected health information. Since that time, because we could not identify what specific information may have been accessed, we reviewed the contents of the affected email box in order to find out: (1) what information was involved, (2) who may have been affected, and (3) where those people resided so that we could provide proper notice. Based upon the investigation, the compromised email account may have contained your: name, address, date of birth, bank account number, Social Security or driver’s license number, and certain health information such as patient account or medical record number, health insurance number, diagnosis(es), provider name, and treatment information.

**What We Are Doing About It**

When we discovered this incident, we immediately disabled the affected email account and had all employees reset their passwords. We also scanned our email system to detect and neutralize any potentially dangerous emails or unauthorized activity. To further enhance our security and help prevent similar occurrences in the future, we have taken or will be taking the following steps:

1. Closely monitoring and restricting outside access to our systems;
2. Increasing the frequency of our password reset policy;
3. Adding two factor authentication to access our network;
4. Strengthening our spam filtering to help block dangerous emails;
5. Updating our response procedures to more quickly and effectively respond to incidents;
6. Enhancing our cyber training and providing regular communications in order to increase cyber awareness;
7. Updating our policies to promptly terminate inactive accounts; and
8. Regularly reviewing email boxes to remove or archive outdated information that we no longer need.

In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to appropriate state and federal regulators.

### **What You Can Do**

Because this incident was an attempt to redirect our funds, we do not believe that the attack was focused on accessing your information. However, in an abundance of caution, we recommend that you take the following preventative measures to help protect your information:

1. Enroll in a complimentary, two-year membership with Experian. This membership will provide you with identity monitoring services, including a copy of your credit report at signup; credit monitoring; identity restoration; Experian IdentityWorks ExtendCARE™; and up to \$1 million in identity theft insurance. Instructions on how to activate your membership are included at the end of this letter.
2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements, free credit reports and health insurance Explanation of Benefits (EOB) forms for any unauthorized or suspicious activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.
3. Report any incidents of unauthorized activity, suspicious activity or suspected identity theft to your local law enforcement, state Attorney General, health insurance carrier, and the major credit bureaus.

### **For More Information**

If you have any questions or concerns about this incident, you may contact us by calling us toll-free at 1-844-224-7435, Monday through Friday, 8:30 a.m. - 4:30 p.m. Eastern.

We are very sorry this incident happened and for any inconvenience you may have experienced. The privacy and security of your information is very important to us and we remain committed to doing everything we can to maintain the confidentiality of your information.

Very truly yours,



**Paula Yarbrough, MBA, SPHR**  
*Chief Financial Officer*

## MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit [www.experian.com/credit-advice/topic-fraud-and-identity-theft.html](http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html) for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at [www.consumer.ftc.gov/features/feature-0014-identity-theft](http://www.consumer.ftc.gov/features/feature-0014-identity-theft). The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

### National Credit Reporting Agencies Contact Information

<b>Equifax</b> P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 <a href="http://www.transunion.com">www.transunion.com</a>
--	---	--

### Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at [www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf](http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

**For Massachusetts residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

### Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at [www.annualcreditreport.com](http://www.annualcreditreport.com).

### Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to all three of the credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

### **Additional Helpful Information**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

If this notice letter states that your financial account number and/or credit or debit card number was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

### **STATE SPECIFIC INFORMATION**

**MASSACHUSETTS residents:** There is no charge for requesting a security freeze, and you have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information.

**NEW YORK residents:** You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State  
Division of Consumer Protection  
1-800-697-1220  
<http://www.dos.ny.gov/consumerprotection>

New York Attorney General  
1-800-771-7755  
<http://www.ag.ny.gov/home.html>

**RHODE ISLAND residents:** You have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Office of the Attorney General  
150 South Main Street  
Providence, RI 02903  
[www.riag.ri.gov](http://www.riag.ri.gov)  
Toll-free: 1-401-274-4400

**ADDITIONAL DETAILS REGARDING YOUR 24-MONTH  
EXPERIAN IDENTITYWORKS MEMBERSHIP:**

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by: December 8, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [www.experianidworks.com/3bcredit](http://www.experianidworks.com/3bcredit)
- Provide your **activation code: <code>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877.288.8057** by **December 8, 2021**. Be prepared to provide engagement number **B018604** as proof of eligibility for the identity restoration services by Experian. A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.288.8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



North East Educational and  
Developmental Support Center

September 30, 2021

<<first>> <<last>>  
<<street>>  
<<city>>, <<state>> <<zip>>

***IMPORTANT INFORMATION – PLEASE REVIEW CAREFULLY  
NOTICE OF DATA SECURITY INCIDENT***

Dear Parent or Guardian of <<first>> <<last>>:

I am writing to tell you about a recent data security incident at North East Educational and Developmental Support Center (“NEEDS”) that may have resulted in unauthorized access to information that we maintain about our current or former employees, their relatives or clients who we treat. **At this time, we have no indication that any of your child’s personal information has been inappropriately used by anyone.** We are providing this notice as a precautionary measure, to inform you of the incident, explain the complimentary services we are offering, and suggest ways that you can help protect your child’s information.

**What Happened**

On July 5, 2021, we learned that a NEEDS’ employee email account had been used in a targeted attempt to complete an unauthorized wire transfer of NEEDS’ money. We successfully detected and responded to the attempt before any payments were redirected. We also worked with cyber security experts so that we could better understand what happened and, more importantly, prevent something like this from happening again.

**What Information Was Involved**

On August 2, 2021, we first discovered that the impacted email account contained protected health information. Since that time, because we could not identify what specific information may have been accessed, we reviewed the contents of the affected email box in order to find out: (1) what information was involved, (2) who may have been affected, and (3) where those people resided so that we could provide proper notice. Based upon the investigation, the compromised email account may have contained your child’s name, address, date of birth, Social Security number, and certain health information such as patient account or medical record number, health insurance number, diagnosis(es), provider name, and treatment information.

**What We Are Doing About It**

When we discovered this incident, we immediately disabled the affected email account and had all employees reset their passwords. We also scanned our email system to detect and neutralize any potentially dangerous emails or unauthorized activity. To further enhance our security and help prevent similar occurrences in the future, we have taken or will be taking the following steps:

1. Closely monitoring and restricting outside access to our systems;
2. Increasing the frequency of our password reset policy;
3. Adding two factor authentication to access our network;
4. Strengthening our spam filtering to help block dangerous emails;
5. Updating our response procedures to more quickly and effectively respond to incidents;
6. Enhancing our cyber training and providing regular communications in order to increase cyber awareness;
7. Updating our policies to promptly terminate inactive accounts; and
8. Regularly reviewing email boxes to remove or archive outdated information that we no longer need.

In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to appropriate state and federal regulators.

### **What You Can Do**

Because this incident was an attempt to redirect our funds, we do not believe that the attack was focused on accessing your child's information. However, in an abundance of caution, we recommend that you take the following preventative measures to help protect your child's information:

1. Enroll your child in a complimentary, one-year membership with Experian. This membership will provide your child with detection and resolution of identity theft, including Social Security number tracing; internet surveillance; identity restoration; Experian IdentityWorks ExtendCARE™; and up to \$1 million in identity theft insurance. Instructions on how to activate your child's membership are included at the end of this letter.
2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your child's account statements, free credit reports and health insurance Explanation of Benefits (EOB) forms for any unauthorized or suspicious activity. Information on additional ways to protect your child's information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.
3. Report any incidents of unauthorized activity, suspicious activity or suspected identity theft to your local law enforcement, state Attorney General, health insurance carrier, and the major credit bureaus.

### **For More Information**

If you have any questions or concerns about this incident, you may contact us by calling us toll-free at 1-844-224-7435, Monday through Friday, 8:30 a.m. - 4:30 p.m. Eastern.

We are very sorry this incident happened and for any inconvenience you or your child may have experienced. The privacy and security of your child's information is very important to us and we remain committed to doing everything we can to maintain the confidentiality of your child's information.

Very truly yours,



**Paula Yarbrough, MBA, SPHR**  
*Chief Financial Officer*

## MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit [www.experian.com/credit-advice/topic-fraud-and-identity-theft.html](http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html) for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at [www.consumer.ftc.gov/features/feature-0014-identity-theft](http://www.consumer.ftc.gov/features/feature-0014-identity-theft). The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

### National Credit Reporting Agencies Contact Information

<b>Equifax</b> P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 <a href="http://www.transunion.com">www.transunion.com</a>
--	---	--

### Obtain Your Child's Credit Report

**In general, minors do not have credit reports. However, if your child is an authorized user or joint account holder of a credit card or other account, he or she may have a legitimate credit history. You can check if a credit report exists for your child by contacting the above-referenced agencies.**

If your child has a credit report, you should monitor it. You may periodically obtain credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at [www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf](http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your child's credit report, if he or she has one.

**For Massachusetts residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If your child has a credit report and you discover inaccurate information or a fraudulent transaction on a credit report, you have the right to request that the consumer reporting agency delete that information from your child's credit report file.

### Place a Fraud Alert on Your Child's Credit File

If your child has a credit report, you may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your child's report and requests that the creditor contact you prior to establishing any new accounts in your child's name. To place a fraud alert on your child's credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at [www.annualcreditreport.com](http://www.annualcreditreport.com).

### Place a Security Freeze on Your Child's Credit File

If your child has a credit report, you may request that a "Security Freeze" be placed on your child's credit file, at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your child's name without consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to all three of the credit reporting agencies listed above.

In order to place the security freeze, you'll need to supply the following information (note that if you are requesting a credit report for your child, this information must be provided for him/her as well, along with your child's birth



certificate and proof of guardianship if your name is not on your child's birth certificate); (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze. If your child has a credit report and you place a security freeze *prior* to enrolling in the credit monitoring services being offered, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your child's credit file.

### **Additional Helpful Information**

Even if you do not find any suspicious activity on your child's initial credit reports, the Federal Trade Commission (FTC) recommends that you check credit reports periodically to help spot problems and address them quickly.

If you find suspicious activity on your child's credit reports or have reason to believe your child's information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve your child of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

If your child's personal information has been used to file a false tax return, to open an account or to attempt to open an account in your child's name, or to commit fraud or other crimes against your child, you may file a police report in the city in which your child currently resides.

### **STATE SPECIFIC INFORMATION**

**MASSACHUSETTS residents:** There is no charge for requesting a security freeze, and you have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information.

**NEW YORK residents:** You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State  
Division of Consumer Protection  
1-800-697-1220  
<http://www.dos.ny.gov/consumerprotection>

New York Attorney General  
1-800-771-7755  
<http://www.ag.ny.gov/home.html>

**RHODE ISLAND residents:** You have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Office of the Attorney General  
150 South Main Street  
Providence, RI 02903  
[www.riag.ri.gov](http://www.riag.ri.gov)  
Toll-free: 1-401-274-4400

**ADDITIONAL DETAILS REGARDING YOUR CHILD'S 12-MONTH  
EXPERIAN IDENTITYWORKS MEMBERSHIP:**

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR CHILD'S PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by: December 8, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code: <code>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877.288.8057** by **December 8, 2021**. Be prepared to provide engagement number **B018605** as proof of eligibility for the identity restoration services by Experian. A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your child's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877.288.8057**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at <http://www.ExperianIDWorks.com/restoration>. You will also find self-help tips and information about identity protection at this site.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



North East Educational and  
Developmental Support Center

September 30, 2021

<<first>> <<last>>  
<<street>>  
<<city>>, <<state>> <<zip>>

***IMPORTANT INFORMATION – PLEASE REVIEW CAREFULLY  
NOTICE OF DATA SECURITY INCIDENT***

Dear <<first>> <<last>>:

I am writing to tell you about a recent data security incident that involved some of the information North East Educational and Developmental Support Center (“NEEDS”) maintains about its current or former employees, their relatives, clients who we treat, or other persons associated with NEEDS. The incident may have involved your bank account number, Social Security number or driver’s license number. **At this time, we have no indication that any of your personal information has been inappropriately used by anyone.** We are providing this notice as a precautionary measure, to inform you of the incident, explain the complimentary services we are offering you, and suggest ways that you can help protect your information.

**What We Are Doing About It**

When we discovered this incident, we immediately took steps to mitigate and remediate the incident. Because cyber threats are always evolving, we evaluate our IT security protocols on a continual basis to make sure that sensitive data is protected to the greatest extent possible. In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to appropriate state and federal regulators.

**What You Can Do**

In an abundance of caution, we recommend that you take the following preventative measures to help protect your information:

1. Enroll in a complimentary, two-year membership with Experian. This membership will provide you with identity monitoring services, including a copy of your credit report at signup; credit monitoring; identity restoration; Experian IdentityWorks ExtendCARE™; and up to \$1 million in identity theft insurance. Instructions on how to activate your membership are included at the end of this letter.
2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized or suspicious activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.

3. Report any incidents of unauthorized activity, suspicious activity or suspected identity theft to your local law enforcement, state Attorney General and the major credit bureaus. **As a Massachusetts resident, you have the right to obtain any police report filed about this incident.** If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it concerning any fraud or identity theft committed using your personal information.

**For More Information**

If you have any questions or concerns about this incident, you may contact us by calling us toll-free at 1-844-224-7435, Monday through Friday, 8:30 a.m. - 4:30 p.m. Eastern.

We are very sorry this incident happened and for any inconvenience you may have experienced. The privacy and security of your information is very important to us and we remain committed to doing everything we can to maintain the confidentiality of your information.

Very truly yours,



**Paula Yarbrough, MBA, SPHR**  
*Chief Financial Officer*

## MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit [www.experian.com/credit-advice/topic-fraud-and-identity-theft.html](http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html) for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at [www.consumer.ftc.gov/features/feature-0014-identity-theft](http://www.consumer.ftc.gov/features/feature-0014-identity-theft). The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

### National Credit Reporting Agencies Contact Information

<b>Equifax</b> P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 <a href="http://www.transunion.com">www.transunion.com</a>
--	---	--

### Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at [www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf](http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

**For Massachusetts residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

### Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at [www.annualcreditreport.com](http://www.annualcreditreport.com).

### Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to all three of the credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative

report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

### **Additional Helpful Information**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

If this notice letter states that your financial account number and/or credit or debit card number was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

**ADDITIONAL DETAILS REGARDING YOUR 24-MONTH  
EXPERIAN IDENTITYWORKS MEMBERSHIP:**

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by: December 8, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [www.experianidworks.com/3bcredit](http://www.experianidworks.com/3bcredit)
- Provide your **activation code: <code>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877.288.8057** by **December 8, 2021**. Be prepared to provide engagement number **B018604** as proof of eligibility for the identity restoration services by Experian. A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.288.8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.