CodeMetro

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

<<Mail ID>>
Parent or Legal Guardian of:
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

To Parent or Legal Guardian of <<Name 1>>:

We are writing to inform you about a data security incident that may have affected your child's information. CodeMetro provides software solutions such as NPAWorks to applied behavior analysis (ABA) providers, including <<Customer Name>>, from which your child may have received services.

What happened?

On April 21, 2020, CodeMetro systems suffered a ransomware attack, which was detected within hours of its deployment. Upon discovery, we took immediate steps to contain the threat and engaged a third-party forensic firm to investigate the incident and assist with remediation efforts. We also notified federal law enforcement authorities of the incident.

Our investigation has found that prior to deploying the ransomware, the criminals were able to access a database server and deploy tools to copy and remove some data. The database server contained health-related patient information.

What information may have been involved?

As a result of the investigation, we were able to determine that your child's personal information may have been involved, and we notified your child's provider of the incident by letter dated May 29, 2020. The patient information may have included: (1) information to identify and contact the patient (such as patient name, patient picture, parent/legal guardian name, guarantor name, address, email address, phone number, date of birth, gender, and ethnicity); (2) school information (school name, Individualized Education Program (IEP) start and review dates, assessment and psychological evaluation dates, and eligibility type (type of behavioral or developmental condition or impairment)); (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount, and policy ID number); and (4) medical information (dates of enrollment with your ABA provider's services, authorized services, allotted time/number of sessions, diagnostic codes and modifiers, charge/reimbursement rates, outcomes, and provider names). Please note that the data fields that may have been impacted depend on the provider and not all data fields may have been involved for all individuals. If your child is covered under TRICARE, the health insurance ID number may be a guarantor/legal guardian's Social Security number.

AA6541 v.client

What we are doing.

As soon as we discovered the incident, we promptly launched a forensic investigation, contacted law enforcement, and took steps to remediate the incident. We take data security incidents very seriously and have worked to implement the necessary steps to ensure the continued protection of your data. In response to this incident, we have enhanced our security and monitoring as well as hardened our systems to minimize the risk of any similar incident in the future.

Because it is possible your TRICARE ID number may be your Social Security number, we have arranged to offer you credit monitoring for a period of one year, at no cost to you, through TransUnion. You have until September 30, 2020 to activate these services, and instructions on how to activate these services are included in the attached Reference Guide.

What you can do.

In addition to signing up for your complimentary credit monitoring, the enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your and your child's personal information. We encourage you to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all of your account activity is valid; any questionable charges should be promptly reported to the provider's billing office, or for insurance statements, to your insurance company.

For more information.

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit www.codemetrotransparency.com, or call toll-free 1-855-907-2106. This call center is open from 9:00 AM to 9:00 PM Eastern time, Monday through Friday, except holidays. We apologize for any concern this incident may cause you and we greatly appreciate your understanding.

We regret that this incident occurred and are very sorry for any distress or inconvenience we may have caused you. We take the privacy of your personal information seriously.

Sincerely,

Jason Cummings
General Manager

CodeMetro
1333 S. Mayflower Avenue, Ste 350
Monrovia, CA 91016

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Enroll in TransUnion 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.)

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. 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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

CodeMetro

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

<<Mail ID>>
Parent or Legal Guardian of:
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

To Parent or Legal Guardian of <<Name 1>>:

We are writing to inform you about a data security incident that may have affected your child's information. CodeMetro provides software solutions such as NPAWorks to applied behavior analysis (ABA) providers, including <<Customer Name>>, from which your child may have received services.

What happened?

On April 21, 2020, CodeMetro systems suffered a ransomware attack, which was detected within hours of its deployment. Upon discovery, we took immediate steps to contain the threat and engaged a third-party forensic firm to investigate the incident and assist with remediation efforts. We also notified federal law enforcement authorities of the incident.

Our investigation has found that prior to deploying the ransomware, the criminals were able to access a database server and deploy tools to copy and remove some data. The database server contained health-related patient information.

What information may have been involved?

As a result of the investigation, we were able to determine that your child's personal information may have been involved, and we notified your child's provider of the incident by letter dated May 29, 2020. The patient information may have included: (1) information to identify and contact the patient (such as patient name, patient picture, parent/legal guardian name, guarantor name, address, email address, phone number, date of birth, gender, and ethnicity); (2) school information (school name, Individualized Education Program (IEP) start and review dates, assessment and psychological evaluation dates, and eligibility type (type of behavioral or developmental condition or impairment)); (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount, and policy ID number); and (4) medical information (dates of enrollment with your ABA provider's services, authorized services, allotted time/number of sessions, diagnostic codes and modifiers, charge/reimbursement rates, outcomes, and provider names). Please note that the data fields that may have been impacted depend on the provider and not all data fields may have been involved for all individuals.

What we are doing.

As soon as we discovered the incident, we promptly launched a forensic investigation, contacted law enforcement, and took steps to remediate the incident. We take data security incidents very seriously and have worked to implement the necessary steps to ensure the continued protection of your data. In response to this incident, we have enhanced our security and monitoring as well as hardened our systems to minimize the risk of any similar incident in the future.

What you can do.

The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your child's personal information. We encourage you to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all of your account activity is valid; any questionable charges should be promptly reported to the provider's billing office, or for insurance statements, to your insurance company.

For more information.

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit www.codemetrotransparency.com, or call toll-free 1-855-907-2106. This call center is open from 9:00 AM to 9:00 PM Eastern time, Monday through Friday, except holidays. We apologize for any concern this incident may cause you and we greatly appreciate your understanding.

We regret that this incident occurred and are very sorry for any distress or inconvenience we may have caused you. We take the privacy of your personal information seriously.

Sincerely,

Jason Cummings
General Manager

CodeMetro
1333 S. Mayflower Avenue, Ste 350
Monrovia, CA 91016

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. 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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

CodeMetro

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

To <<Name 1>>:

We are writing to inform you about a data security incident that may have affected some of your personal information. CodeMetro provides software solutions such as NPAWorks to applied behavior analysis (ABA) providers, including your current (or former) employer, <<Customer Name>>.

What happened?

On April 21, 2020, CodeMetro systems suffered a ransomware attack, which was detected within hours of its deployment. Upon discovery, we took immediate steps to contain the threat and engaged a third-party forensic firm to investigate the incident and assist with remediation efforts. We also notified federal law enforcement authorities of the incident.

Our investigation has found that prior to deploying the ransomware, the criminals were able to access a database server and deploy tools to copy and remove some data. The database server contained employee payroll information.

What information may have been involved?

As a result of the investigation, we were able to determine that your personal information may have been involved, and we notified your employer of the incident on May 29, 2020. The employee information may have included: name, address, Social Security number (SSN), driver's license number, and date of birth.

What we are doing.

As soon as we discovered the incident, we promptly launched a forensic investigation, contacted law enforcement, and took steps to remediate the incident. We take data security incidents very seriously and have worked to implement the necessary steps to ensure the continued protection of your data. In response to this incident, we have enhanced our security and monitoring as well as hardened our systems to minimize the risk of any similar incident in the future.

We have arranged to offer you credit monitoring for a period of one year, at no cost to you, through TransUnion. You have until September 30, 2020 to activate these services, and instructions on how to activate these services are included in the attached Reference Guide.

What you can do.

In addition to signing up for your complimentary credit monitoring, the enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to carefully review credit reports and account statements to ensure that all of your account activity is valid; any questionable charges should be promptly reported to the company with which the account is maintained.

For more information.

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit www.codemetrotransparency.com, or call toll-free 1-855-907-2106. This call center is open from 9:00 AM to 9:00 PM Eastern time, Monday through Friday, except holidays. We apologize for any concern this incident may cause you and we greatly appreciate your understanding.

We regret that this incident occurred and are very sorry for any distress or inconvenience we may have caused you. We take the privacy of your personal information seriously.

Sincerely,

Jason Cummings
General Manager

CodeMetro
1333 S. Mayflower Avenue, Ste 350
Monrovia, CA 91016

Reference Guide

Review Your Account Statements

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Enroll in TransUnion 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.)

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. 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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of Iowa

You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at:

Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowaattorneygeneral.gov.

For Residents of Maryland

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, http://www.marylandattorneygeneral.gov/.

For Residents of New Mexico

New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For Residents of New York

You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For Residents of Oregon

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us.

CodeMetro

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>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Notice of Data Breach

To <<Name 1>>:

We are writing to inform you about a data security incident that may have affected your information. CodeMetro provides software solutions such as NPAWorks to applied behavior analysis (ABA) providers, including <<Customer Name>>, from which you may have received services.

What happened?

On April 21, 2020, CodeMetro systems suffered a ransomware attack, which was detected within hours of its deployment. Upon discovery, we took immediate steps to contain the threat and engaged a third-party forensic firm to investigate the incident and assist with remediation efforts. We also notified federal law enforcement authorities of the incident.

Our investigation has found that prior to deploying the ransomware, the criminals were able to access a database server and deploy tools to copy and remove some data. The database server contained health-related patient information.

What information may have been involved?

As a result of the investigation, we were able to determine that your personal information may have been involved, and we notified your provider of the incident by letter dated May 29, 2020. The patient information may have included: (1) information to identify and contact the patient (such as patient name, patient picture, parent/legal guardian name, guarantor name, address, email address, phone number, date of birth, gender, and ethnicity); (2) school information (school name, Individualized Education Program (IEP) start and review dates, assessment and psychological evaluation dates, and eligibility type (type of behavioral or developmental condition or impairment)); (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount, and policy ID number); and (4) medical information (dates of enrollment with your ABA provider’s services, authorized services, allotted time/number of sessions, diagnostic codes and modifiers, charge/reimbursement rates, outcomes, and provider names). Please note that the data fields that may have been impacted depend on the provider and not all data fields may have been involved for all individuals.

What we are doing.

As soon as we discovered the incident, we promptly launched a forensic investigation, contacted law enforcement, and took steps to remediate the incident. We take data security incidents very seriously and have worked to implement the necessary steps to ensure the continued protection of your data. In response to this incident, we have enhanced our security and monitoring as well as hardened our systems to minimize the risk of any similar incident in the future.

What you can do.

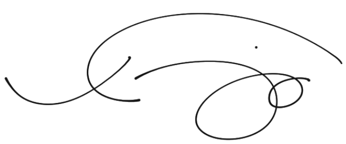
The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all of your account activity is valid; any questionable charges should be promptly reported to the provider's billing office, or for insurance statements, to your insurance company.

For more information.

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit www.codemetrotransparency.com, or call toll-free 1-855-907-2106. This call center is open from 9:00 AM to 9:00 PM Eastern time, Monday through Friday, except holidays. We apologize for any concern this incident may cause you and we greatly appreciate your understanding.

We regret that this incident occurred and are very sorry for any distress or inconvenience we may have caused you. We take the privacy of your personal information seriously.

Sincerely,



Jason Cummings
General Manager

CodeMetro
1333 S. Mayflower Avenue, Ste 350
Monrovia, CA 91016

AA6622 v.client

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. 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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

CodeMetro

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

<<Mail ID>>
Parent or Legal Guardian of:
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

To Parent or Legal Guardian of <<Name 1>>:

We are writing to inform you about a data security incident that may have affected your child's information. CodeMetro provides software solutions such as NPAWorks to applied behavior analysis providers, including Learning Solutions Kids, Inc., from which your child may have received services.

What happened?

On April 21, 2020, CodeMetro systems suffered a ransomware attack, which was detected within hours of its deployment. Upon discovery, we took immediate steps to contain the threat and engaged a third-party forensic firm to investigate the incident and assist with remediation efforts. We also notified federal law enforcement authorities of the incident.

Our investigation has found that prior to deploying the ransomware, the criminals were able to access a database server and deploy tools to copy and remove some data. The database server contained health-related patient information.

What information may have been involved?

As a result of the investigation, we were able to determine that your child's personal information may have been involved, and we notified your child's provider of the incident by letter dated May 29, 2020. The patient information may have included: name, address, parent/legal guardian name, parent/legal guardian address, email address, and phone number.

What we are doing.

As soon as we discovered the incident, we promptly launched a forensic investigation, contacted law enforcement, and took steps to remediate the incident. We take data security incidents very seriously and have worked to implement the necessary steps to ensure the continued protection of your data. In response to this incident, we have enhanced our security and monitoring as well as hardened our systems to minimize the risk of any similar incident in the future.

What you can do.

The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your child's personal information. We encourage you to carefully review credit reports and account statements sent from providers as well as your insurance company to ensure that all of your account activity is valid; any questionable charges should be promptly reported to the provider's billing office, or for insurance statements, to your insurance company.

For more information.

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit www.codemetrotransparency.com, or call toll-free 1-855-907-2106. This call center is open from 9:00 AM to 9:00 PM Eastern time, Monday through Friday, except holidays. We apologize for any concern this incident may cause you and we greatly appreciate your understanding.

We regret that this incident occurred and are very sorry for any distress or inconvenience we may have caused you. We take the privacy of your personal information seriously.

Sincerely,

Jason Cummings
General Manager

CodeMetro
1333 S. Mayflower Avenue, Ste 350
Monrovia, CA 91016

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. 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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

CodeMetro

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

<<Mail ID>>
Padre o tutor legal de:
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<u>Notificación sobre violación de datos</u>

Estimado padre o tutor legal de <<Name 1>>:

Le escribimos para informarle acerca de un incidente de seguridad de datos que pudo haber afectado la información de su hijo. CodeMetro brinda soluciones de software como NPAWorks a proveedores de análisis conductual aplicado (ACA), incluido <<CUSTOMER NAME>>, de quien su hijo podría haber obtenido servicios.

¿Qué ocurrió?

El 21 de abril de 2020, los sistemas de CodeMetro sufrieron un ataque de ransomware, que se detectó horas después de haber ocurrido. Al descubrirlo, tomamos medidas inmediatamente para contener la amenaza y contratamos a una empresa forense externa para investigar el incidente, y ayudar en los esfuerzos de remediación. También notificamos del incidente a las autoridades de cumplimiento de la ley federales.

Mediante nuestra investigación, se encontró que antes de ocurrir el ransomware, los criminales pudieron acceder al servidor de la base de datos y usar herramientas para copiar y eliminar algunos datos. El servidor de la base de datos contenía información de salud de pacientes.

¿Qué información puede haber estado involucrada?

Como resultado de la investigación, pudimos determinar que es posible que la información personal de su hijo haya estado involucrada, y notificamos al prestador de su hijo sobre el incidente mediante una carta con fecha 29 de mayo de 2020. La información de los pacientes puede haber incluido: (1) información para identificar y comunicarse con el paciente (como por ejemplo, nombre del paciente, fotografía del paciente, nombre de padre/tutor legal, nombre del garante, domicilio, dirección de correo electrónico, número de teléfono, fecha de nacimiento, género y origen étnico); (2) información escolar (nombre de la escuela, fechas de inicio y revisión del Programa de Educación Individualizado (PEI), fechas de evaluación y análisis psicológico, y tipo de elegibilidad (tipo de afección o discapacidad conductual o del desarrollo)); (3) información del seguro de salud (nombre del pagador, fechas del contrato del pagador, información de la póliza, incluido tipo y monto del deducible, y número de ID de la póliza); y (4) información médica (fechas de inscripción en los servicios de su proveedor de ACA, servicios autorizados, tiempo/cantidad de sesiones asignadas, códigos y modificadores de diagnóstico, tarifas de cargos/reembolsos, resultados y nombres de proveedores). Tenga en cuenta que los campos de datos que pueden haber sido impactados dependen del proveedor y es posible que no todos los campos de datos hayan estado involucrados para todas las personas. Si su hijo tiene cobertura de TRICARE, el número de ID del seguro de salud podría ser el número de Seguro Social de un garante/tutor legal.

¿Qué estamos haciendo?

Apenas detectamos el incidente, iniciamos inmediatamente una investigación forense, nos comunicamos con las autoridades de cumplimiento de la ley y tomamos medidas para solucionarlo. Tomamos muy en serio los incidentes de seguridad de datos y hemos trabajado para implementar las medidas necesarias para garantizar la protección continua de sus datos. Como respuesta a este incidente, hemos mejorado nuestra seguridad y monitoreo, y hemos fortalecido nuestros sistemas para minimizar el riesgo de incidentes similares en el futuro.

Dado que es posible que su número de ID de TRICARE sea su número de Seguro Social, hemos acordado ofrecerle monitoreo crediticio por un año, sin ningún costo para usted, a través de TransUnion. Usted tiene plazo hasta el 30 Septiembre 2020 para activar estos servicios, y las instrucciones de cómo activarlos se incluyen en la Guía de referencia adjunta.

¿Qué puede hacer usted?

Además de la inscripción para su monitoreo electrónico sin cargo, la Guía de referencia adjunta incluye información adicional acerca de las medidas generales que puede tomar para monitorear y proteger su información personal y la de su hijo. Las personas deben revisar con cuidado sus informes crediticios y los estados de cuenta que les envían los proveedores y su compañía de seguro para asegurarse de que toda la actividad de sus cuentas sea válida; los cargos cuestionables se deben informar inmediatamente a la oficina de facturación del proveedor o, para los estados de cuenta del seguro, a la compañía de seguro.

Para obtener más información.

Si tiene alguna pregunta sobre este asunto o le gustaría obtener información adicional, consulte la Guía de referencia adjunta, ingrese a www.codemetrotransparency.com o llame al 1-855-907-2106. Este centro de llamadas esta abierto de 9:00 a.m. a 9:00 p.m., hora del este de lunes a viernes, excepto feriados. Le pedimos disculpas por las preocupaciones que pueda causarle este incidente y apreciamos su comprensión.

Lamentamos que haya ocurrido este incidente y lamentamos las preocupaciones o los inconvenientes que le pudiera haber provocado. Tomamos la privacidad de su información personal seriamente.

Atentamente,

Jason Cummings
Gerente general

CodeMetro
1333 S. Mayflower Avenue, Ste 350
Monrovia, CA 91016

Guía de referencia

Revise sus estados de cuenta

Revise con cuidado los estados de cuenta que le envían los proveedores y su compañía de seguro para asegurarse de que toda su actividad de cuenta sea válida. Informe los cargos cuestionables inmediatamente a la oficina de facturación del proveedor o, para los estados de cuenta del seguro, a su compañía de seguro.

Proporcione toda la información personal actualizada a su proveedor de atención médica

Es posible que en la oficina de su proveedor de atención médica se le pida una identificación con foto para verificar su identidad. Si es posible, traiga una identificación con foto con usted a cada cita. Es posible que en la oficina de su proveedor también se le pida que confirme su fecha de nacimiento, domicilio, teléfono y otra información pertinente para poder asegurarse de que toda su información esté actualizada. Asegúrese de avisar a la oficina de su proveedor cuando haya cambios en su información. Revisar con atención esta información en la oficina de su proveedor en cada visita puede ayudar a evitar problemas y abordarlos rápidamente si hubiera alguna discrepancia.

Solicite su informe crediticio anual gratuito

Para solicitar su informe crediticio anual gratuito, visite www.annualcreditreport.com, llame gratis al 1-877-322-8228 o complete el Formulario de solicitud de informe crediticio anual en el sitio web de la Comisión Federal de Comercio (Federal Trade Commission, FTC) de los Estados Unidos, www.ftc.gov, y envíelo por correo a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Las tres agencias de crédito brindan informes crediticios anuales gratuitos únicamente a través del sitio web, el número gratuito o el formulario de solicitud.

Al recibir su informe crediticio, revíselo detenidamente. Busque cuentas que no haya abierto. Busque en la sección "Preguntas" nombres de acreedores a los que no haya solicitado crédito. Algunas compañías cobran con nombres que no son los de su tienda o sus nombres comerciales; la oficina de crédito podrá saber si ese es el caso. Busque en la sección "información personal" si hay imprecisiones en la información (por ejemplo, el domicilio particular y el número de Seguro Social).

Si ve algo que no entiende, llame a la oficina de crédito al teléfono que figura en el informe. Los errores pueden ser una señal de alerta de un posible robo de identidad. Notifique a las oficinas de crédito acerca de cualquier imprecisión en su informe, ya sea debido a error o fraude, lo antes posible para que se pueda investigar la información y, si fuera un error, corregirla. Si hay cuentas o cargos que no autorizó, notifique inmediatamente a la oficina de crédito correspondiente por teléfono y por escrito. La información que no se puede explicar también debe ser informada a la policía local o la oficina del sheriff, dado que puede ser indicio de alguna actividad delictiva.

Cómo inscribirse en TransUnion Servicio de supervisión crediticia *my*TrueIdentity de cortesía durante un año

Como garantía, hemos acordado que usted se inscriba, sin costo alguno, en un servicio de supervisión crediticia en línea (*my*TrueIdentity) durante un año proporcionado por TransUnion Interactive, una subsidiaria de TransUnion®, una de las tres empresas de informes crediticios a nivel nacional.

Cómo inscribirse: Puede inscribirse en línea o vía entrega por correo postal de EE. UU.

- Para inscribirse en este servicio, visite el sitio web de *my*TrueIdentity en **www.MyTrueIdentity.com** y en el espacio indicado como "Enter Activation Code" **<<Ingresar código de activación>>**, ingrese el código de activación de 12 letras **<<Insert Unique 12-letter Activation Code>>** y siga los tres pasos para recibir su servicio de supervisión crediticia en línea en minutos.

- Si no tiene acceso a Internet y desea inscribirse en un servicio de supervisión crediticia similar fuera de línea e impreso, vía entrega por correo postal de EE. UU., llame a la línea gratuita de Servicios de respuesta por fraudes de TransUnion al **1-855-288-5422**. Cuando se le solicite, ingrese el código de pase telefónico de seis dígitos **<<Insert static 6-digit Telephone Pass Code>>** y siga los pasos para inscribirse en el servicio de supervisión crediticia fuera de línea, agregar una alerta de fraude inicial a su expediente de crédito o hablar con un representante de TransUnion si considera que puede ser una víctima del robo de identidad.

Puede inscribirse en el servicio de supervisión crediticia en línea o fuera de línea en cualquier momento a partir de ahora y hasta el **<<Enrollment Deadline>>**. Debido a las leyes de privacidad, no podemos inscribirlo(a) directamente. Tenga en cuenta que es posible que los servicios de supervisión crediticia no estén disponibles para personas que no tengan un expediente de crédito con TransUnion o una dirección en los Estados Unidos (o sus territorios) y un número de Seguro Social válido. Inscribirse en este servicio no afectará su calificación crediticia.

DETALLES ADICIONALES RELACIONADOS CON SU SERVICIO DE SUPERVISIÓN CREDITICIA DE CORTESÍA DURANTE 12 MESES:

- Una vez inscrito, podrá obtener un año de acceso ilimitado a su informe crediticio y su calificación crediticia de TransUnion.
- El servicio de supervisión crediticia diario le notificará si se realiza algún cambio crucial en su expediente de crédito en TransUnion, lo que incluye alertas de fraude, consultas nuevas, cuentas nuevas, nuevos registros públicos, pagos retrasados, cambio de dirección y más.
- El servicio también incluye un acceso al programa de restauración de identidad que brinda asistencia en caso de que su identidad se vea comprometida, y hasta $1.000.000 en seguro contra robo de identidad sin deducible. (Se pueden aplicar restricciones y exclusiones de la póliza).

Le recomendamos aprovechar estas protecciones y estar atento a incidentes de fraude y robo de identidad, lo que incluye revisar y monitorear regularmente sus informes crediticios y estados de cuenta.

<u>Comuníquese con la Comisión Federal de Comercio de los Estados Unidos</u>

Si detecta operaciones no autorizadas en cualquiera de sus cuentas financieras, notifique inmediatamente a la compañía de la tarjeta de pago o institución financiera correspondiente. Si detecta incidentes de robo de identidad o fraude, informe inmediatamente a las autoridades de cumplimiento de la ley locales, al fiscal general de su estado y a la FTC.

Puede comunicarse con la FTC para saber más acerca de cómo protegerse de convertirse en víctima de robo de identidad mediante la siguiente información de contacto:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

<u>Implemente una alerta de fraude en su expediente de crédito</u>

Para protegerse contra un posible robo de identidad, considere incorporar una alerta de fraude en su expediente de crédito. Una alerta de fraude ayuda a evitar la posibilidad de que un ladrón de identidad abra nuevas cuentas de crédito a su nombre. Cuando un otorgante de crédito verifica el historial crediticio de alguien que solicita un crédito, el otorgante obtiene una notificación de que el solicitante podría ser víctima de robo de identidad. La alerta notifica al otorgante del crédito que tome medidas para verificar la identidad del solicitante. Puede incorporar una alerta de fraude en su informe crediticio llamando a uno de los números gratuitos de fraude que se indican a continuación. Se comunicará con un sistema telefónico automatizado que permite marcar su expediente con una alerta de fraude en las tres oficinas de crédito.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

<u>Bloqueos de seguridad</u>

Usted tiene derecho a solicitar que se coloque un bloqueo crediticio por parte de una agencia de informes del consumidor, sin cargo, para que no se puedan abrir créditos nuevos a su nombre sin el uso de un número PIN que se le emite cuando inicia un bloqueo. El bloqueo de seguridad está diseñado para impedir que posibles entidades crediticias accedan a su informe de crédito sin su consentimiento. Si coloca un bloqueo de seguridad, los posibles acreedores y otros terceros no podrán acceder a su informe crediticio, a menos que suspenda temporalmente el bloqueo. Por lo tanto, el uso de un bloqueo de seguridad puede dilatar su capacidad de obtener crédito.

A diferencia de la alerta de fraude, el bloqueo de seguridad de su archivo crediticio debe ser implementado en cada oficina de crédito por separado. Para colocar un bloqueo de seguridad en su informe crediticio, debe comunicarse con la agencia de informe crediticio por teléfono, correo o un medio electrónico seguro, y proporcionar los datos de identificación de su identidad. Debe incluir la siguiente información al solicitar un bloqueo de seguridad (tenga en cuenta que si solicita un informe crediticio para su cónyuge, debe informar de ello al titular): (1) nombre completo con inicial del segundo nombre y cualquier sufijo, si lo usa; (2) número de Seguro Social; (3) fecha de nacimiento; (4) domicilio actual y cualquier domicilio previo de los últimos cinco años; (5) cualquier queja o denuncia de incidente que corresponda y se haya hecho ante una agencia de cumplimiento de la ley o el Registro de Automotores. La solicitud también debe incluir la copia de una tarjeta de identificación emitida por el gobierno y la copia de una factura reciente de servicios públicos o el estado de cuenta bancario o del seguro. Es fundamental que cada copia sea legible, muestre su nombre y dirección de correo postal actual, y la fecha de emisión.

A continuación, encontrará la información de contacto correspondiente para las tres agencias de informes del consumidor:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Una vez que haya enviado su solicitud, la agencia de informe crediticio debe implementar el bloqueo de seguridad dentro del plazo de 1 día hábil después de recibir la solicitud por teléfono o medio electrónico seguro, y dentro de los 3 días hábiles después de recibir la solicitud por correo. Dentro de los cinco días hábiles después de colocar el bloqueo de seguridad, la agencia de informe crediticio enviará su confirmación e información acerca de cómo puede eliminar el bloqueo en el futuro.

Para residentes de Carolina del Norte

También puede obtener información sobre cómo prevenir y evitar el robo de identidad en la oficina del fiscal general de Carolina del Norte:

North Carolina Attorney General’s Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

CodeMetro

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

<<Mail ID>>
Padre o tutor legal de:
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Notificación sobre violación de datos

Estimado padre o tutor legal de <<Name 1>>:

Le escribimos para informarle acerca de un incidente de seguridad de datos que pudo haber afectado la información de su hijo. CodeMetro brinda soluciones de software como NPAWorks a proveedores de análisis conductual aplicado (ACA), incluido <<CUSTOMER NAME>>, de quien su hijo podría haber obtenido servicios.

¿Qué ocurrió?

El 21 de abril de 2020, los sistemas de CodeMetro sufrieron un ataque de ransomware, que se detectó horas después de haber ocurrido. Al descubrirlo, tomamos medidas inmediatamente para contener la amenaza y contratamos a una empresa forense externa para investigar el incidente, y ayudar en los esfuerzos de remediación. También notificamos del incidente a las autoridades de cumplimiento de la ley federales.

Mediante nuestra investigación, se encontró que antes de ocurrir el ransomware, los criminales pudieron acceder al servidor de la base de datos y usar herramientas para copiar y eliminar algunos datos. El servidor de la base de datos contenía información de salud de pacientes.

¿Qué información puede haber estado involucrada?

Como resultado de la investigación, pudimos determinar que es posible que la información personal de su hijo haya estado involucrada, y notificamos al prestador de su hijo sobre el incidente mediante una carta con fecha 29 de mayo de 2020. La información de los pacientes puede haber incluido: (1) información para identificar y comunicarse con el paciente (como por ejemplo, nombre del paciente, fotografía del paciente, nombre de padre/tutor legal, nombre del garante, domicilio, dirección de correo electrónico, número de teléfono, fecha de nacimiento, género y origen étnico); (2) información escolar (nombre de la escuela, fechas de inicio y revisión del Programa de Educación Individualizado (PEI), fechas de evaluación y análisis psicológico, y tipo de elegibilidad (tipo de afección o discapacidad conductual o del desarrollo)); (3) información del seguro de salud (nombre del pagador, fechas del contrato del pagador, información de la póliza, incluido tipo y monto del deducible, y número de ID de la póliza); y (4) información médica (fechas de inscripción en los servicios de su proveedor de ACA, servicios autorizados, tiempo/cantidad de sesiones asignadas, códigos y modificadores de diagnóstico, tarifas de cargos/reembolsos, resultados y nombres de proveedores). Tenga en cuenta que los campos de datos que pueden haber sido impactados dependen del proveedor y es posible que no todos los campos de datos hayan estado involucrados para todas las personas.

¿Qué es proveedor de soluciones de software tamos haciendo?

Apenas detectamos el incidente, iniciamos inmediatamente una investigación forense, nos comunicamos con las autoridades de cumplimiento de la ley y tomamos medidas para solucionarlo. Tomamos muy en serio los incidentes de seguridad de datos y hemos trabajado para implementar las medidas necesarias para garantizar la protección continua de sus datos. Como respuesta a este incidente, hemos mejorado nuestra seguridad y monitoreo, y hemos fortalecido nuestros sistemas para minimizar el riesgo de incidentes similares en el futuro.

¿Qué puede hacer usted?

La Guía de referencia adjunta incluye información adicional acerca de las medidas generales que puede tomar para monitorear y proteger la información personal de su hijo. Las personas deben revisar con cuidado sus informes crediticios y los estados de cuenta que les envían los proveedores y su compañía de seguro para asegurarse de que toda la actividad de sus cuentas sea válida; los cargos cuestionables se deben informar inmediatamente a la oficina de facturación del proveedor o, para los estados de cuenta del seguro, a la compañía de seguro.

Para obtener más información.

Si tiene alguna pregunta sobre este asunto o le gustaría obtener información adicional, consulte la Guía de referencia adjunta, ingrese a www.codemetrotransparency.com o llame al 1-855-907-2106. Este centro de llamadas esta abierto de 9:00 a.m. a 9:00 p.m., hora del este de lunes a viernes, excepto feriados. Le pedimos disculpas por las preocupaciones que pueda causarle este incidente y apreciamos su comprensión.

Lamentamos que haya ocurrido este incidente y lamentamos las preocupaciones o los inconvenientes que le pudiera haber provocado. Tomamos la privacidad de su información personal seriamente.

Atentamente,

Jason Cummings
Gerente general

CodeMetro
1333 S. Mayflower Avenue, Ste 350
Monrovia, CA 91016

AA6652 v.clientv02

Guía de referencia

Revise sus estados de cuenta

Revise con cuidado los estados de cuenta que le envían los proveedores y su compañía de seguro para asegurarse de que toda su actividad de cuenta sea válida. Informe los cargos cuestionables inmediatamente a la oficina de facturación del proveedor o, para los estados de cuenta del seguro, a su compañía de seguro.

Proporcione toda la información personal actualizada a su proveedor de atención médica

Es posible que en la oficina de su proveedor de atención médica se le pida una identificación con foto para verificar su identidad. Si es posible, traiga una identificación con foto con usted a cada cita. Es posible que en la oficina de su proveedor también se le pida que confirme su fecha de nacimiento, domicilio, teléfono y otra información pertinente para poder asegurarse de que toda su información esté actualizada. Asegúrese de avisar a la oficina de su proveedor cuando haya cambios en su información. Revisar con atención esta información en la oficina de su proveedor en cada visita puede ayudar a evitar problemas y abordarlos rápidamente si hubiera alguna discrepancia.

Solicite su informe crediticio anual gratuito

Para solicitar su informe crediticio anual gratuito, visite www.annualcreditreport.com, llame gratis al 1-877-322-8228 o complete el Formulario de solicitud de informe crediticio anual en el sitio web de la Comisión Federal de Comercio (Federal Trade Commission, FTC) de los Estados Unidos, www.ftc.gov, y envíelo por correo a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Las tres agencias de crédito brindan informes crediticios anuales gratuitos únicamente a través del sitio web, el número gratuito o el formulario de solicitud.

Al recibir su informe crediticio, revíselo detenidamente. Busque cuentas que no haya abierto. Busque en la sección “Preguntas” nombres de acreedores a los que no haya solicitado crédito. Algunas compañías cobran con nombres que no son los de su tienda o sus nombres comerciales; la oficina de crédito podrá saber si ese es el caso. Busque en la sección “información personal” si hay imprecisiones en la información (por ejemplo, el domicilio particular y el número de Seguro Social).

Si ve algo que no entiende, llame a la oficina de crédito al teléfono que figura en el informe. Los errores pueden ser una señal de alerta de un posible robo de identidad. Notifique a las oficinas de crédito acerca de cualquier imprecisión en su informe, ya sea debido a error o fraude, lo antes posible para que se pueda investigar la información y, si fuera un error, corregirla. Si hay cuentas o cargos que no autorizó, notifique inmediatamente a la oficina de crédito correspondiente por teléfono y por escrito. La información que no se puede explicar también debe ser informada a la policía local o la oficina del sheriff, dado que puede ser indicio de alguna actividad delictiva.

Comuníquese con la Comisión Federal de Comercio de los Estados Unidos

Si detecta operaciones no autorizadas en cualquiera de sus cuentas financieras, notifique inmediatamente a la compañía de la tarjeta de pago o institución financiera correspondiente. Si detecta incidentes de robo de identidad o fraude, informe inmediatamente a las autoridades de cumplimiento de la ley locales, al fiscal general de su estado y a la FTC.

Puede comunicarse con la FTC para saber más acerca de cómo protegerse de convertirse en víctima de robo de identidad mediante la siguiente información de contacto:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Implemente una alerta de fraude en su expediente de crédito

Para protegerse contra un posible robo de identidad, considere incorporar una alerta de fraude en su expediente de crédito. Una alerta de fraude ayuda a evitar la posibilidad de que un ladrón de identidad abra nuevas cuentas de crédito a su nombre. Cuando un otorgante de crédito verifica el historial crediticio de alguien que solicita un crédito, el otorgante obtiene una notificación de que el solicitante podría ser víctima de robo de identidad. La alerta notifica al otorgante del crédito que tome medidas para verificar la identidad del solicitante. Puede incorporar una alerta de fraude en su informe crediticio llamando a uno de los números gratuitos de fraude que se indican a continuación. Se comunicará con un sistema telefónico automatizado que permite marcar su expediente con una alerta de fraude en las tres oficinas de crédito.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Bloqueos de seguridad

Usted tiene derecho a solicitar que se coloque un bloqueo crediticio por parte de una agencia de informes del consumidor, sin cargo, para que no se puedan abrir créditos nuevos a su nombre sin el uso de un número PIN que se le emite cuando inicia un bloqueo. El bloqueo de seguridad está diseñado para impedir que posibles entidades crediticias accedan a su informe de crédito sin su consentimiento. Si coloca un bloqueo de seguridad, los posibles acreedores y otros terceros no podrán acceder a su informe crediticio, a menos que suspenda temporalmente el bloqueo. Por lo tanto, el uso de un bloqueo de seguridad puede dilatar su capacidad de obtener crédito.

A diferencia de la alerta de fraude, el bloqueo de seguridad de su archivo crediticio debe ser implementado en cada oficina de crédito por separado. Para colocar un bloqueo de seguridad en su informe crediticio, debe comunicarse con la agencia de informe crediticio por teléfono, correo o un medio electrónico seguro, y proporcionar los datos de identificación de su identidad. Debe incluir la siguiente información al solicitar un bloqueo de seguridad (tenga en cuenta que si solicita un informe crediticio para su cónyuge, debe informar de ello al titular): (1) nombre completo con inicial del segundo nombre y cualquier sufijo, si lo usa; (2) número de Seguro Social; (3) fecha de nacimiento; (4) domicilio actual y cualquier domicilio previo de los últimos cinco años; (5) cualquier queja o denuncia de incidente que corresponda y se haya hecho ante una agencia de cumplimiento de la ley o el Registro de Automotores. La solicitud también debe incluir la copia de una tarjeta de identificación emitida por el gobierno y la copia de una factura reciente de servicios públicos o el estado de cuenta bancario o del seguro. Es fundamental que cada copia sea legible, muestre su nombre y dirección de correo postal actual, y la fecha de emisión.

A continuación, encontrará la información de contacto correspondiente para las tres agencias de informes del consumidor:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Una vez que haya enviado su solicitud, la agencia de informe crediticio debe implementar el bloqueo de seguridad dentro del plazo de 1 día hábil después de recibir la solicitud por teléfono o medio electrónico seguro, y dentro de los 3 días hábiles después de recibir la solicitud por correo. Dentro de los cinco días hábiles después de colocar el bloqueo de seguridad, la agencia de informe crediticio enviará su confirmación e información acerca de cómo puede eliminar el bloqueo en el futuro.

Para residentes de Carolina del Norte

También puede obtener información sobre cómo prevenir y evitar el robo de identidad en la oficina del fiscal general de Carolina del Norte:

North Carolina Attorney General’s Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

CodeMetro

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>>

Notificación sobre violación de datos

Estimado <<Name 1>>:

Le escribimos para informarle acerca de un incidente de seguridad de datos que pudo haber afectado su información. CodeMetro brinda soluciones de software como NPAWorks a proveedores de análisis conductual aplicado (ACA), incluido <<CUSTOMER NAME>>, de quien podría haber obtenido servicios.

¿Qué ocurrió?

El 21 de abril de 2020, los sistemas de CodeMetro sufrieron un ataque de ransomware, que se detectó horas después de haber ocurrido. Al descubrirlo, tomamos medidas inmediatamente para contener la amenaza y contratamos a una empresa forense externa para investigar el incidente, y ayudar en los esfuerzos de remediación. También notificamos del incidente a las autoridades de cumplimiento de la ley federales.

Mediante nuestra investigación, se encontró que antes de ocurrir el ransomware, los criminales pudieron acceder al servidor de la base de datos y usar herramientas para copiar y eliminar algunos datos. El servidor de la base de datos contenía información de salud de pacientes.

¿Qué información puede haber estado involucrada?

Como resultado de la investigación, pudimos determinar que es posible que su información personal haya estado involucrada, y notificamos a su prestador sobre el incidente mediante una carta con fecha 29 de mayo de 2020. La información de los pacientes que puede haber incluido: (1) información para identificar y comunicarse con el paciente (como por ejemplo, nombre del paciente, fotografía del paciente, nombre de padre/tutor legal, nombre del garante, domicilio, dirección de correo electrónico, número de teléfono, fecha de nacimiento, género y origen étnico); (2) información escolar (nombre de la escuela, fechas de inicio y revisión del Programa de Educación Individualizado (PEI), fechas de evaluación y análisis psicológico, y tipo de elegibilidad (tipo de afección o discapacidad conductual o del desarrollo)); (3) información del seguro de salud (nombre del pagador, fechas del contrato del pagador, información de la póliza, incluido tipo y monto del deducible, y número de ID de la póliza); y (4) información médica (fechas de inscripción en los servicios de su proveedor de ACA, servicios autorizados, tiempo/cantidad de sesiones asignadas, códigos y modificadores de diagnóstico, tarifas de cargos/reembolsos, resultados y nombres de proveedores). Tenga en cuenta que los campos de datos que pueden haber sido impactados dependen del proveedor y es posible que no todos los campos de datos hayan estado involucrados para todas las personas.

¿Qué es proveedor de soluciones de software tamos haciendo?

Apenas detectamos el incidente, iniciamos inmediatamente una investigación forense, nos comunicamos con las autoridades de cumplimiento de la ley y tomamos medidas para solucionarlo. Tomamos muy en serio los incidentes de seguridad de datos y hemos trabajado para implementar las medidas necesarias para garantizar la protección continua de sus datos. Como respuesta a este incidente, hemos mejorado nuestra seguridad y monitoreo, y hemos fortalecido nuestros sistemas para minimizar el riesgo de incidentes similares en el futuro.

¿Qué puede hacer usted?

La Guía de referencia adjunta incluye información adicional acerca de las medidas generales que puede tomar para monitorear y proteger su información personal. Las personas deben revisar con cuidado sus informes crediticios y los estados de cuenta que les envían los proveedores y su compañía de seguro para asegurarse de que toda la actividad de sus cuentas sea válida; los cargos cuestionables se deben informar inmediatamente a la oficina de facturación del proveedor o, para los estados de cuenta del seguro, a la compañía de seguro.

Para obtener más información.

Si tiene alguna pregunta sobre este asunto o le gustaría obtener información adicional, consulte la Guía de referencia adjunta, ingrese a www.codemetrotransparency.com o llame al 1-855-907-2106. Este centro de llamadas esta abierto de 9:00 a.m. a 9:00 p.m., hora del este de lunes a viernes, excepto feriados. Le pedimos disculpas por las preocupaciones que pueda causarle este incidente y apreciamos su comprensión.

Lamentamos que haya ocurrido este incidente y lamentamos las preocupaciones o los inconvenientes que le pudiera haber provocado. Tomamos la privacidad de su información personal seriamente.

Atentamente,

Jason Cummings
Gerente general

CodeMetro
1333 S. Mayflower Avenue, Ste 350
Monrovia, CA 91016

Guía de referencia

Revise sus estados de cuenta

Revise con cuidado los estados de cuenta que le envían los proveedores y su compañía de seguro para asegurarse de que toda su actividad de cuenta sea válida. Informe los cargos cuestionables inmediatamente a la oficina de facturación del proveedor o, para los estados de cuenta del seguro, a su compañía de seguro.

Proporcione toda la información personal actualizada a su proveedor de atención médica

Es posible que en la oficina de su proveedor de atención médica se le pida una identificación con foto para verificar su identidad. Si es posible, traiga una identificación con foto con usted a cada cita. Es posible que en la oficina de su proveedor también se le pida que confirme su fecha de nacimiento, domicilio, teléfono y otra información pertinente para poder asegurarse de que toda su información esté actualizada. Asegúrese de avisar a la oficina de su proveedor cuando haya cambios en su información. Revisar con atención esta información en la oficina de su proveedor en cada visita puede ayudar a evitar problemas y abordarlos rápidamente si hubiera alguna discrepancia.

Solicite su informe crediticio anual gratuito

Para solicitar su informe crediticio anual gratuito, visite www.annualcreditreport.com, llame gratis al 1-877-322-8228 o complete el Formulario de solicitud de informe crediticio anual en el sitio web de la Comisión Federal de Comercio (Federal Trade Commission, FTC) de los Estados Unidos, www.ftc.gov, y envíelo por correo a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Las tres agencias de crédito brindan informes crediticios anuales gratuitos únicamente a través del sitio web, el número gratuito o el formulario de solicitud.

Al recibir su informe crediticio, revíselo detenidamente. Busque cuentas que no haya abierto. Busque en la sección "Preguntas" nombres de acreedores a los que no haya solicitado crédito. Algunas compañías cobran con nombres que no son los de su tienda o sus nombres comerciales; la oficina de crédito podrá saber si ese es el caso. Busque en la sección "información personal" si hay imprecisiones en la información (por ejemplo, el domicilio particular y el número de Seguro Social).

Si ve algo que no entiende, llame a la oficina de crédito al teléfono que figura en el informe. Los errores pueden ser una señal de alerta de un posible robo de identidad. Notifique a las oficinas de crédito acerca de cualquier imprecisión en su informe, ya sea debido a error o fraude, lo antes posible para que se pueda investigar la información y, si fuera un error, corregirla. Si hay cuentas o cargos que no autorizó, notifique inmediatamente a la oficina de crédito correspondiente por teléfono y por escrito. La información que no se puede explicar también debe ser informada a la policía local o la oficina del sheriff, dado que puede ser indicio de alguna actividad delictiva.

Comuníquese con la Comisión Federal de Comercio de los Estados Unidos

Si detecta operaciones no autorizadas en cualquiera de sus cuentas financieras, notifique inmediatamente a la compañía de la tarjeta de pago o institución financiera correspondiente. Si detecta incidentes de robo de identidad o fraude, informe inmediatamente a las autoridades de cumplimiento de la ley locales, al fiscal general de su estado y a la FTC.

Puede comunicarse con la FTC para saber más acerca de cómo protegerse de convertirse en víctima de robo de identidad mediante la siguiente información de contacto:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Implemente una alerta de fraude en su expediente de crédito

Para protegerse contra un posible robo de identidad, considere incorporar una alerta de fraude en su expediente de crédito. Una alerta de fraude ayuda a evitar la posibilidad de que un ladrón de identidad abra nuevas cuentas de crédito a su nombre. Cuando un otorgante de crédito verifica el historial crediticio de alguien que solicita un crédito, el otorgante obtiene una notificación de que el solicitante podría ser víctima de robo de identidad. La alerta notifica al otorgante del crédito que tome medidas para verificar la identidad del solicitante. Puede incorporar una alerta de fraude en su informe crediticio llamando a uno de los números gratuitos de fraude que se indican a continuación. Se comunicará con un sistema telefónico automatizado que permite marcar su expediente con una alerta de fraude en las tres oficinas de crédito.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Bloqueos de seguridad

Usted tiene derecho a solicitar que se coloque un bloqueo crediticio por parte de una agencia de informes del consumidor, sin cargo, para que no se puedan abrir créditos nuevos a su nombre sin el uso de un número PIN que se le emite cuando inicia un bloqueo. El bloqueo de seguridad está diseñado para impedir que posibles entidades crediticias accedan a su informe de crédito sin su consentimiento. Si coloca un bloqueo de seguridad, los posibles acreedores y otros terceros no podrán acceder a su informe crediticio, a menos que suspenda temporalmente el bloqueo. Por lo tanto, el uso de un bloqueo de seguridad puede dilatar su capacidad de obtener crédito.

A diferencia de la alerta de fraude, el bloqueo de seguridad de su archivo crediticio debe ser implementado en cada oficina de crédito por separado. Para colocar un bloqueo de seguridad en su informe crediticio, debe comunicarse con la agencia de informe crediticio por teléfono, correo o un medio electrónico seguro, y proporcionar los datos de identificación de su identidad. Debe incluir la siguiente información al solicitar un bloqueo de seguridad (tenga en cuenta que si solicita un informe crediticio para su cónyuge, debe informar de ello al titular): (1) nombre completo con inicial del segundo nombre y cualquier sufijo, si lo usa; (2) número de Seguro Social; (3) fecha de nacimiento; (4) domicilio actual y cualquier domicilio previo de los últimos cinco años; (5) cualquier queja o denuncia de incidente que corresponda y se haya hecho ante una agencia de cumplimiento de la ley o el Registro de Automotores. La solicitud también debe incluir la copia de una tarjeta de identificación emitida por el gobierno y la copia de una factura reciente de servicios públicos o el estado de cuenta bancario o del seguro. Es fundamental que cada copia sea legible, muestre su nombre y dirección de correo postal actual, y la fecha de emisión.

A continuación, encontrará la información de contacto correspondiente para las tres agencias de informes del consumidor:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Una vez que haya enviado su solicitud, la agencia de informe crediticio debe implementar el bloqueo de seguridad dentro del plazo de 1 día hábil después de recibir la solicitud por teléfono o medio electrónico seguro, y dentro de los 3 días hábiles después de recibir la solicitud por correo. Dentro de los cinco días hábiles después de colocar el bloqueo de seguridad, la agencia de informe crediticio enviará su confirmación e información acerca de cómo puede eliminar el bloqueo en el futuro.

Para residentes de Carolina del Norte

También puede obtener información sobre cómo prevenir y evitar el robo de identidad en la oficina del fiscal general de Carolina del Norte:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov