Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 25, 2022

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event - Correction

Dear Sir or Madam:

We represent Consumers Supply Distributing, LLC ("CSD"), located at 718 N Derby Ln, North Sioux City, SD 57049. On February 25, 2022, our office submitted a Notice of Data Event to your office on behalf of CSD. The notice incorrectly stated that CSD provided a proactive notification of the event to employees on February 25, 2022; however, that preliminary notification was actually sent on **January 27, 2022**. Attached as ***Exhibit AA*** is the prior submitted notification for your reference. To reiterate, the only change to the prior submitted notification is the date that CSD provided proactive notification of the event. All other information in the submission remains unchanged.

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/aml
Enclosure

EXHIBIT AA

From: Samantha Myers
Sent: Friday, February 25, 2022 12:45 PM
To: consumer@ag.iowa.gov
Cc: Sian Schafle; John Mullen; Alyssa Lopez
Subject: Consumers Supply Distributing LLC - Notice of Data Event - IA
Attachments: CSD - Notice of Data Event - IA.pdf

Good afternoon,

Please see attached notice of data event on behalf of our client, Consumers Supply Distributing, LLC.

Thank you,
Sami

Samantha Myers
Attorney
Mullen Coughlin LLC
426 W. Lancaster Avenue, Suite 200
Devon, PA 19333
(267) 930-1266 - Office
(484) 643-3761 - Mobile
smyers@mullen.law

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 25, 2022

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Consumers Supply Distributing, LLC ("CSD") located at 718 N Derby Ln, North Sioux City, SD 57049, and are writing to notify your office of an incident that may affect the security of some personal information relating to seven hundred ninety-two (792) Iowa residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, CSD does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

On January 21, 2022, CSD identified unusual activity on its network and began an investigation. On January 23, 2022, the investigation determined that an unauthorized actor accessed the CSD network and removed certain files from CSD systems. The investigation determined that the unauthorized actor accessed CSD's network from January 16, 2022 to January 21, 2022. Upon confirmation that the unauthorized actor gained access to CSD's network, out of an abundance of caution, on February 25, 2022 CSD proactively notified its employee population of the incident via email and offered complimentary credit monitoring to any employee wishing to enroll. A copy of the notice provided to employees is attached here as ***Exhibit A***.

Following notification to employee, CSD reviewed the potentially affected systems to determine what specific sensitive information they contain and to whom the information related. Following that review, CSD worked to obtain appropriate contact information for potentially impacted

individuals. That review concluded on February 11, 2022, at which point CSD put resources in place to notify potentially impacted individuals via mail.

The personal information as defined by Iowa Code Ann. § 715C.1(11)(a) that could have been subject to unauthorized access includes, Social Security number, and financial account information.

Notice to Iowa Residents

On or about February 25, 2022, CSD provided written notice of this incident to affected individuals, which includes seven hundred ninety-two (792) Iowa residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, CSD moved quickly to investigate and respond to the incident, assess the security of CSD systems, and identify potentially affected individuals. Further, CSD notified federal law enforcement regarding the event. CSD is providing access to credit monitoring services for one (1) year, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, CSD is providing impacted individuals with guidance on how to better protect against identity theft and fraud. CSD is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. CSD is also providing information regarding best practices with respect to password reuse and rotation of passwords for personal accounts.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,

Sian M Schafle.

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/aml
Enclosure

EXHIBIT A

Dear Consumers Supply Employees,

As you may be aware, Consumers Supply Distributing, LLC ("Consumers") recently detected suspicious activity on its network. As a precautionary measure, we took our systems offline and began to investigate the incident. We are working with third-party subject matter specialists to investigate the nature and scope of this incident.

However, as you are our valued employees, we write to provide you with general information and best practices so that you may evaluate for yourself whether to take any action. Specifically, below we discuss password recommendations, and at the end of this email we included further resources and guidance for individuals to protect their information. Please note that our ongoing investigation is working to confirm the nature of this event, including impact to data. We will update you shortly on the investigation and we will notify those involved consistent with applicable law.

Regarding passwords, while our investigation is ongoing, as a precautionary measure, we recommend that you change your passwords for any personal or business online accounts that you may have accessed while on your personal or company device or workstation or may have stored in your web browser. Best practice is to ensure you are changing any password(s) using a Consumers device and that you use complex different passwords for all of your accounts.

Further, given that many people often use the same password for many accounts, we are also encouraging you to take this opportunity to change the passwords for any personal accounts which would share the same or similar credentials as the accounts you may have accessed from any company devices.

In addition, and as an added precaution, you may also enroll in the complimentary identity credit monitoring services we are making available to you. Enrollment instructions are attached to this letter. Please contact Cecily Johnston to obtain your unique credit monitoring code. The activation deadline for enrollment is May 31, 2022.

Please know that safeguarding the information in our care remains a top priority. We appreciate your patience as we work to resolve these issues. Should you have any questions, please contact Cecily Johnston or Dan Patee.

Sincerely – CSD Management

General Guidance and Best Practices

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud and to monitor your account statements and credit reports. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You may also contact the three credit reporting agencies and request a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. As an alternative to a security freeze, you can place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. Contact information for the credit reporting agencies is below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Reset Online Account Passwords

As a general practice, we encourage individuals to frequently reset online account passwords, to use complex password combinations, and to not share passwords or use identical passwords for multiple online accounts.

Additional Information

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

The Federal Trade Commission can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

EXHIBIT B

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>>

Re: <<Variable Header>>

Dear <<Name1>>:

Consumers Supply Distributing, LLC ("CSD") is writing to make you aware of an incident that may affect the security of some of your information. We take this incident seriously and write to provide you with information about the incident, what we are doing in response, and the resources that are available to you to help better protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? On January 21, 2022, CSD identified unusual activity on its network and began an investigation. On January 23, 2022, the investigation determined that an unauthorized actor accessed the CSD network and removed certain files from CSD systems. Based on information known to date, the investigation determined that the unauthorized actor accessed CSD's network from January 16, 2022 to January 21, 2022. CSD reviewed the potentially affected systems to determine what sensitive information they contain and to whom the information related. Following that review, CSD worked to obtain appropriate contact information for potentially impacted individuals. That review concluded on February 11, 2022, at which point CSD put resources in place to notify potentially impacted individuals, including you.

What Information Was Involved? In general, CSD stores employee information on our systems including name, date of birth, employee identification number, financial account information, medical information related to absences from work, health insurance information, and Social Security number. Therefore, it is possible some of this information may have been affected by this incident if you or someone on your behalf provided this information to CSD.

What We Are Doing. We take this incident and the security of information within our care seriously. Upon discovery of this incident, we launched an in-depth investigation with the assistance of third-party forensic investigators to determine the full nature and scope of this incident. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our existing policies and procedures and implementing additional safeguards to further secure the information in our systems as appropriate. Although our investigation is ongoing, we notified law enforcement and are notifying regulatory authorities as required by law. We are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. As an added precaution, we arranged to have Equifax provide credit monitoring services for <<CM Length>> at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Personal Information*." You may also enroll in the complimentary identity protection and credit monitoring services we are making available to you. Enrollment instructions are attached to this letter.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please call our dedicated assistance line at 855-604-1819 Monday through Friday 9:00 am – 9:00 pm Eastern Time (excluding major U.S. holidays).

Sincerely,

Consumers Supply Distributing, LLC

Steps You Can Take to Help Protect Personal Information

Enroll in Credit Monitoring

EQUIFAX®

Enter your Activation Code: <<*ACTIVATION CODE*>>
Enrollment Deadline: <<*Enrollment Deadline*>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***.

Enter your unique Activation Code of ***<<ACTIVATION CODE>>*** then click "Submit" and follow these 4 steps:

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

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

---

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

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

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

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

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

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

As a general practice, we encourage individuals to frequently reset online account passwords, to use complex password combinations, and to not share passwords or use identical passwords for multiple online accounts. You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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

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

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

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

Re: <<Variable Header>>

Dear Parent or Guardian of <<Name1>>:

Consumers Supply Distributing, LLC ("CSD") is writing to make you aware of an incident that may affect the security of some of your minor's information. We take this incident seriously, and write to provide you with information about the incident, what we are doing in response, and the resources that are available to you to help better protect your minor's personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? On January 21, 2022, CSD identified unusual activity on its network and began an investigation with the assistance of third-party forensic specialists. On January 23, 2022, the investigation determined that an unauthorized actor accessed the CSD network and removed certain files from CSD systems. Based on information known to date, the investigation determined that the unauthorized actor accessed CSD's network from January 16, 2022 to January 21, 2022. CSD reviewed the potentially affected systems to determine what sensitive information they contain and to whom the information related. Following that review, CSD worked to obtain appropriate contact information for potentially impacted individuals. That review concluded on February 11, 2022, at which point CSD put resources in place to notify potentially impacted individuals.

What Information Was Involved? In general, CSD stores employee information on our systems including name, date of birth, employee identification number, financial account information, medical information related to absences from work, health insurance information, and Social Security number. Therefore, it is possible some of your minor's information may have been affected by this incident if you have provided this information to CSD.

What We Are Doing. We take this incident and the security of information within our care seriously. Upon discovery of this incident, we launched an in-depth investigation with the assistance of third-party forensic investigators to determine the full nature and scope of this incident. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our existing policies and procedures and implementing additional safeguards to further secure the information in our systems as appropriate. Although our investigation is ongoing, we notified law enforcement and are notifying regulatory authorities as required by law. We are also notifying potentially affected individuals so that you may take further steps to best protect your minor's personal information, should you feel it is appropriate to do so. As an added precaution, we arranged to have Equifax provide child monitoring services for <<Cm Length>> at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your minor's account statements and monitoring free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Personal Information*." You may also enroll your minor in the complimentary child monitoring services we are making available to you. Enrollment instructions are attached to this letter.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please call our dedicated assistance line at 855-604-1819 Monday through Friday 9:00 am – 9:00 pm Eastern Time (excluding major U.S. holidays).

Sincerely,

Consumers Supply Distributing, LLC

Steps You Can Take to Help Protect Personal Information

Enroll in Minor Monitoring Services

EQUIFAX®

Enter your Activation Code: <<*ACTIVATION CODE*>>
Enrollment Deadline: <<*Enrollment Deadline*>>

Equifax Child Monitoring Package *(for Equifax Credit Watch™ Gold members)*

Key Features

- Child Monitoring for up to four children under the age of 18
- Emailed notifications of activity on the child's Equifax credit report

Enrollment Instructions

Parent/guardian, after completing your enrollment in Equifax Credit Watch™ Gold:

Return to ***www.equifax.com/activate***.

Enter your unique Activation Code of ***<<ACTIVATION CODE>>*** for Equifax Child Monitoring Package, then click "Submit" and follow these additional steps.

1. **Sign In:**
   Click the 'Sign in here' link under the "Let's get started" header.
   Sign in with your email address and password you created when initially creating your account.
2. **Checkout**:
   Click 'Sign Me Up' to finish your enrollment.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features and enroll minor children.

How to Add Minors to Your Equifax Child Monitoring Package

You will be able to add minors to your Equifax Child Monitoring Package through your product dashboard.

1. Sign in to your account to access the "Your People" module on your dashboard.
2. Click the link to "Add a Child."
3. From there, enter your child's first name, last name, date of birth and social security number.
   Repeat steps for each minor child (up to four).

   Equifax will then create an Equifax credit file for your child, lock it and then alert you if there is any activity on that child's Equifax credit file. You can add up to 4 children under the age of 18 with your Equifax Child Monitoring Package.

Monitor Your Accounts

Typically, a minor under the age of eighteen does not have credit in his or her name, and the consumer reporting agencies do not have a credit report in a minor's name. To find out if your minor has a credit report, or to request a manual search for your minor's Social Security number, each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone or in writing or you may visit the below websites.

Under U.S. law, individuals with credit are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of a credit report should your minor have established credit.

Adults and minors sixteen years or older have the right to place a "security freeze" on a credit report, which will prohibit a consumer reporting agency from releasing information in the credit report without express authorization. A parent or guardian also has the right to place a "security freeze" on a minor's credit report if the child is under the age of sixteen. This right includes proactively placing a "security freeze" on a minor's credit report if the minor is under sixteen years old. If the nationwide credit reporting agencies do not have a credit file on the minor, they will create one so they can freeze it. This record cannot be used for credit purposes. It is there to make sure the child's record is frozen and protected against potential identity theft and fraud. Pursuant to federal law, you cannot be charged to place or lift a security freeze on a credit report. Should you wish to place a security freeze on a credit file or proactively place a freeze on a minor's credit report, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-349-9960
www.experian.com/freeze/center.html	**www.transunion.com/credit-freeze**	www.equifax.com/personal/credit-report-services

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

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

To request information about the existence of a credit file in your minor's name, search for your minor's Social Security number, place a security freeze on your minor's credit file, place a fraud alert on your minor's credit report (if one exists), or request a copy of your minor's credit report you may be required to provide the following information:

- A driver's license or another government issued identification card, such as a state ID card, etc.;
- proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
- a copy of your minor's birth certificate;
- a copy of your minor's Social Security card;
- your minor's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- your minor's date of birth; and previous addresses for the past two years.

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

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

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

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