

Via Electronic Mail to: idtheft@oag.state.md.us

February 16, 2024

Anthony G. Brown, Attorney General
Office of the Attorney General, State of Maryland
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: **Notice of Security Incident**

Dear Attorney General Brown:

This letter is to provide you with information regarding unauthorized access or use of personal information involving Maryland residents ("impacted individuals"). CareFirst BlueCross Blue Shield Community Health Plan-District of Columbia ("CareFirst CHPDC"), a former District of Columbia Medicaid Care Organization, is providing you with information regarding the unauthorized access or use as required by Maryland Code §14-3501 et seq.

CareFirst CHPDC is a wholly owned subsidiary of Trusted Health Plans, Inc. Trusted Health Plans, Inc. is a wholly owned subsidiary of the CareFirst, Inc. insurance holding company system (CareFirst).

What Happened

On December 15, 2023, we learned that a CareFirst CHPDC website, hosted by a third-party vendor, had an unprotected Uniform Resource Locator (URL) or commonly known as a website address that allowed the URL to be available to the public. Upon accessing this URL, a data file automatically began downloading ("Security Event"). On December 18, 2023, CareFirst CHPDC determined that the data file contained protected health information ("PHI") and personally identifiable information ("PII").

On January 2, 2024, CareFirst CHPDC determined that logs used to track access to the website showed multiple computers accessed the URL while it was publicly available and likely downloaded the data file.

This incident **is not** indicative of threat actor activity targeting CareFirst or any of our subsidiaries. This is also **not** indicative of any compromise of internal CareFirst or CareFirst CHPDC infrastructure or services and does not represent any ongoing threat to our systems.

CareFirst CHPDC acted promptly and secured the URL by removing it from public access so no further access to the data could be made. To further protect the information, we eliminated the ability for it to be found using search engines such as Google.com, ending the risk that the information could be accessed.



This program is funded in part by the Government of the District of Columbia Department of Health Care Finance.

The impacted individuals include former enrollees of CareFirst CHPDC between 2016 and 2023, CareFirst members of BlueCross BlueShield and its subsidiaries and healthcare providers. The information may have included the full name, address, telephone number, email address, date of birth, Medicaid identification number, claim identification number, provider name and, in very limited instances, clinical information, for 28 Maryland residents. The information also included the social security number and/or taxpayer identification number, whichever number is used for tax purpose, of 34 Maryland healthcare providers.

While we do not have any evidence that the information has been misused, to help protect their identity, we are offering a free two (2) year membership in Experian's® IdentityWorksSM.

CareFirst CHPDC takes the security of its and its customers' data extremely seriously. We will be notifying the affected individuals and have provided you with sample notices. If you have any questions or concerns, please contact me at Todd.Cioni@carefirst.com or by phone at 410-528-7170.

Sincerely,



P. Todd Cioni
Vice President, Chief Compliance, Ethics and Privacy Officer

Enclosure

**CareFirst BlueCross BlueShield
Community Health Plan
District of Columbia**

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589



K8641-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

PARENT OR GUARDIAN OF
SAMPLE A SAMPLE - L01 MINOR



APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY



February 16, 2024

Re: Notice of Security Event

Dear Parent or Guardian of Sample A. Sample:

CareFirst BlueCross BlueShield Community Health Plan District of Columbia (CareFirst CHPDC), formerly Trusted Health Plan, is writing to notify you about an event that may have impacted your child's information. We want you to know what we are doing to help protect your child and how you can also help protect their information.

Why am I receiving this letter

You are receiving this letter because your child was an enrollee of CareFirst CHPDC between 2016 and 2023.

What Happened

On December 15, 2023, we learned that a CareFirst CHPDC website, hosted by a third-party vendor, contained an unprotected Uniform Resource Locator (URL); commonly known as a website address, allowing the URL to be publicly available. When a user accessed this URL, a data file automatically began downloading ("Security Event"). On December 18, 2023, CareFirst CHPDC determined that the data file contained protected health information ("PHI").

On January 2, 2024, CareFirst CHPDC determined that logs used to track access to the website showed multiple computers accessed the URL while it was publicly available and likely downloaded the data file.

CareFirst CHPDC has notified the D.C. Department of Health Care Finance (DHCF) regarding the Security Event.

What Information Was Publicly Available

The publicly available information may have included personal information about your child, such as their full name, address, telephone number, email address, date of birth, Medicaid identification number, claim identification number, provider name and, in very limited instances, clinical information.

The information **did not** include your child's social security number, banking, or other financial information. We do not have any evidence that your child's information has been misused.



This program is funded in part by the Government of the District of Columbia Department of Health Care Finance.

CareFirst BlueCross BlueShield Community Health Plan District of Columbia is an independent licensee of the Blue Cross and Blue Shield Association. BLUE CROSS®, BLUE SHIELD® and the Cross and Shield Symbols are registered service marks of the Blue Cross and Blue Shield Association, an association of independent Blue Cross and Blue Shield Plans.

0000001



What We Are Doing

When CareFirst CHPDC learned about the Security Event, we immediately took action to secure the URL preventing further access to the information. To further protect your child's information, we removed the URL from public access and eliminated the ability for it to be found using search engines such as Google.com, ending the risk that the information could be accessed. CareFirst CHPDC hired a contractor to help with our data analysis, and we provided regular updates to DHCF's program oversight leadership, Chief Information and Data Protection Officers.

While we do not have any evidence that your child's information has been misused, to help protect their identity, we are offering a free two (2) year membership in Experian's® IdentityWorksSM. This product monitors the creation of a credit file in your child's name and provides detection and theft resolution. This product also includes insurance and identity restoration.

A credit card is not required for enrollment in Experian's® IdentityWorksSM.

To activate your child's membership, please follow the steps below:

- Ensure that you enroll by: May 31, 2024 (Your code will not work after this date.)
- Visit the Experian IdentityWorksSM website to enroll: <https://www.experianidworks.com/minorplus>
- Provide your activation code: ABCDEFGHI
- Provide your minor's information when prompted

Please do not share this information. These links and codes are only for your child.

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian's® IdentityWorksSM online, please contact the customer care team at **833-918-1123** by May 31, 2024. Please be prepared to provide engagement number **B116434** to enroll at no cost.

What You Can Do

There are other things you can do to protect your child from identity theft. Please read the information we have attached to learn more.

For More Information

We are committed to protecting your privacy. **CareFirst CHPDC will not contact you or your child by email or phone about this event. If you receive inquiries by phone, email, text or social media that say they are about this event, they are not from us.** Do not click on any links in email messages or provide any personal information in response.

If you have questions, please contact Experian at 833-918-1123 from 9 a.m. - 9 p.m. Eastern Time, Monday through Friday, except holidays. You can also reach us by email at chpdanswers@carefirst.com or by mail at CHPDC Privacy Office, P.O. Box 14858, Lexington, KY 40512.

You can also find enrollment information and other information about this incident at www.carefirstchpdc.com.

Sincerely,



Cleveland E. Slade
Interim President & CEO
CareFirst Community Health Plan, District of Columbia

INFORMATION ABOUT IDENTITY THEFT PROTECTION

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also obtain a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-888-Equifax (1-888-378-4329), www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1 (800) 916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports. We also recommend that you promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission (FTC). You may contact the FTC or the Washington, DC Office of the Attorney General to obtain additional information.

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW,
Washington, DC 20580, (1-877-IDTHEFT [1-877-438-4338]; TDD: 1-866-653-4261; or www.ftc.gov/idtheft).

Fraud Alerts: For increased protection you may place a fraud alert on your credit file. Such an alert will prompt creditors to contact you before they open any new credit or make changes to your account. There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof.

An extended fraud alert stays on your credit report for 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, 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 credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Placing, lifting, and/or removing a credit freeze from your account is completely free and will not affect your credit score. Please contact the three national credit reporting agencies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com/freeze
TransUnion: P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com/credit-freeze

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the three national credit reporting agencies listed above.



The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day, and year); current address and previous addresses for the past 5 years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state, or military ID card, and a copy of a utility bill, bank, or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

For residents of the District of Columbia: You may also contact the District of Columbia Office of the Attorney General: Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001, (202) 442-9828, <https://oag.dc.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, www.oag.state.md.us.

**CareFirst BlueCross BlueShield
Community Health Plan
District of Columbia**

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589



K8641-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L02 INDIVIDUAL

APT ABC

123 ANY STREET

ANYTOWN, FC 1A2 B3C

COUNTRY



February 16, 2024

Re: Notice of Security Event

Dear Sample A. Sample:

CareFirst BlueCross BlueShield Community Health Plan District of Columbia (CareFirst CHPDC), formerly Trusted Health Plan, is writing to inform you about an event that may have impacted your information. We want you to know what we are doing to help protect you and how you can help protect yourself.

Why am I receiving this letter

You are receiving this letter because you were an enrollee of CareFirst CHPDC between 2016 and 2023.

What Happened

On December 15, 2023, we learned that a CareFirst CHPDC website, hosted by a third-party vendor, contained an unprotected Uniform Resource Locator (URL); commonly known as a website address, allowing the URL to be publicly available. When a user accessed this URL, a data file automatically began downloading ("Security Event"). On December 18, 2023, CareFirst CHPDC determined that the data file contained protected health information ("PHI").

On January 2, 2024, CareFirst CHPDC determined that logs used to track access to the website showed multiple computers accessed the URL while it was publicly available and likely downloaded the data file.

CareFirst CHPDC has notified the D.C. Department of Health Care Finance (DHCF) regarding the Security Event.

What Information Was Publicly Available

The publicly available information may have included personal information about you, such as your full name, address, telephone number, email address, date of birth, Medicaid identification number, claim identification number, provider name and, in very limited instances, clinical information.

The information **did not** include your social security number, banking or other financial information. We do not have any evidence that your information has been misused.



This program is funded in part by the Government of the District of Columbia Department of Health Care Finance.

CareFirst BlueCross BlueShield Community Health Plan District of Columbia is an independent licensee of the Blue Cross and Blue Shield Association. BLUE CROSS®, BLUE SHIELD® and the Cross and Shield Symbols are registered service marks of the Blue Cross and Blue Shield Association, an association of independent Blue Cross and Blue Shield Plans.

0000002



What We Are Doing

When CareFirst CHPDC learned about the Security Event, we immediately took action to secure the URL preventing further access to the information. To further protect your information, we removed the URL from public access and eliminated the ability for it to be found using search engines such as Google.com, ending the risk that the information could be accessed. CareFirst CHPDC hired a contractor to help with our data analysis, and we provided regular updates to DHCF's program oversight leadership, Chief Information and Data Protection Officers.

While we do not have any evidence that your information has been misused, to help protect your identity, we are offering a free two (2) year membership in Experian's® IdentityWorksSM. This product monitors all three credit bureaus, helps detect possible misuse of your personal information and provides detection and theft resolution. This product also includes insurance and identity restoration.

A credit card is not required for enrollment in Experian's® IdentityWorksSM.

To activate your membership, please follow the steps below:

- Ensure that you enroll by: May 31, 2024 (Your code will not work after this date.)
- Visit the Experian's® IdentityWorksSM website to enroll: <https://www.experianidworks.com/credit>
- Provide your activation code: ABCDEFGHI

Please do not share this information. These links and codes are only for you.

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian's® IdentityWorksSM online, please contact the customer care team at **833-918-1123** by May 31, 2024. Please be prepared to provide engagement number **B116369**.

What You Can Do

There are other things you can do to protect yourself from identity theft. Please read the information we have attached to learn more.

For More Information

We are committed to protecting your privacy. **CareFirst CHPDC will not contact you by email or phone about this event. If you receive inquiries by phone, email, text or social media that say they are about this event, they are not from us.** Do not click on any links in email messages or provide any personal information in response.

If you have questions, please contact Experian at 833-918-1123 from 9 a.m. - 9 p.m. Eastern Time, Monday through Friday, except holidays. You can also reach us by email at chpdcanswers@carefirst.com or by mail at CHPDC Privacy Office, P.O. Box 14858, Lexington, KY 40512.

You can also find enrollment information and other information about this incident at www.carefirstchpdc.com.

Sincerely,



Cleveland E. Slade
Interim President & CEO
CareFirst Community Health Plan, District of Columbia

INFORMATION ABOUT IDENTITY THEFT PROTECTION

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also obtain a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-888-Equifax (1-888-378-4329),
www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1 (800) 916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports. We also recommend that you promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission (FTC). You may contact the FTC or the Washington, DC Office of the Attorney General to obtain additional information.

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW,
Washington, DC 20580, (1-877-IDTHEFT [1-877-438-4338]; TDD: 1-866-653-4261; or www.ftc.gov/idtheft).

Fraud Alerts: For increased protection you may place a fraud alert on your credit file. Such an alert will prompt creditors to contact you before they open any new credit or make changes to your account. There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof.

An extended fraud alert stays on your credit report for 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, 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 credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Placing, lifting, and/or removing a credit freeze from your account is completely free and will not affect your credit score. Please contact the three national credit reporting agencies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com/freeze
TransUnion: P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com/credit-freeze



You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the three national credit reporting agencies listed above.

The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day, and year); current address and previous addresses for the past 5 years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state, or military ID card, and a copy of a utility bill, bank, or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

For residents of the District of Columbia: You may also contact the District of Columbia Office of the Attorney General: Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001, (202) 442-9828, <https://oag.dc.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, www.oag.state.md.us.

<Date>

<NAME>

<Address>

<Address>

<City>, <State> <Zip>

Notice of Security Event

Dear <NAME>

CareFirst BlueCross BlueShield Community Health Plan District of Columbia (CareFirst CHPDC), formerly Trusted Health Plan, is writing to tell you about an event that may have impacted your information. We want you to know what we are doing to protect you and how you can protect yourself.

What Happened

On December 15, 2023, we learned that a CareFirst CHPDC website, hosted by a third-party vendor, had an unprotected Uniform Resource Locator (URL) or commonly known as a website address that allowed the URL to be available to the public. Upon accessing this URL, a data file automatically began downloading ("Security Event"). On December 18, 2023, CareFirst CHPDC determined that the data file contained personal and/or business information about your business.

On January 2, 2024, CareFirst CHPDC determined that logs used to track access to the website showed multiple computers accessed the URL while it was publicly available and likely downloaded the data file.

CHPDC has notified the D.C. Department of Health Care Finance (DHCF).

What Information Was Publicly Available

CHPDC determined that there were multiple "forms" hosted on the CHPDC website during its history, in addition to a free text "contact us" form. When these forms were completed, the data was transmitted to the third-party vendor's data warehouse. The information inputted by any individual into those forms were recorded and retained into the transaction log data file that was available on the unprotected URL. The information may have included personal and/or business information about your business, such as the full name of the individual imputing information, business name, business address, National Provider Identifier, tax identification number.

The information **did not** include your banking information. We do not have any evidence that your data has been misused.



This program is funded in part by the Government of the District of Columbia Department of Health Care Finance.

What We Are Doing

When we learned about the Security Event, we immediately took action to secure the URL so no further access to the data could be made. To further protect your data, we removed the URL from public access and eliminated the ability for it to be found using search engines such as Google.com, ending the risk that the data could be accessed. CareFirst CHPDC hired a contractor to help with our data analysis, and provided regular updates to DHCF's program oversight leadership, Chief Information and Data Protection Officers.

What You Can Do

There are other things you can do to protect yourself from identity theft. Please read the information we have attached to learn more.

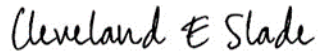
For More Information

We are committed to protecting your privacy. CareFirst CHPDC **will not** contact you by email or phone about this event. If you receive inquiries by phone, email, text or social media that say they are about this event, they are not from us. Do not click on any links in email messages or provide any personal information in response.

If you have questions, please contact Experian at 833-918-1123 from 9 a.m. - 9 p.m. Eastern Time, Monday through Friday, except holidays. You can also reach us by email at chpdcanswers@carefirst.com or by mail at CHPDC Privacy Office, P.O. Box 14858, Lexington, KY 40512.

You can also find other information about this incident at www.carefirstchpdc.com.

Sincerely,



Cleveland E. Slade
Interim President & CEO
CareFirst Community Health Plan, District of Columbia

INFORMATION ABOUT IDENTITY THEFT PROTECTION

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also obtain a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-888-Equifax (1-888-378-4329), www.equifax.com

Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion: P.O. Box 1000, Chester, PA 19022, 1 (800) 916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports. We also recommend that you promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission (FTC). You may contact the FTC or the Washington, DC Office of the Attorney General to obtain additional information.

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, (1-877-IDTHEFT [1-877-438-4338]; TDD: 1-866-653-4261; or www.ftc.gov/idtheft).

Fraud Alerts: For increased protection you may place a fraud alert on your credit file. Such an alert will prompt creditors to contact you before they open any new credit or make changes to your account. There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof.

An extended fraud alert stays on your credit report for 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com

Experian: 1-888-397-3742, www.experian.com

TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, 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 credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Placing, lifting, and/or removing a credit freeze from your account is completely free and will not affect your credit score. Please contact the three national credit reporting agencies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com/freeze
TransUnion: P.O. Box 2000, Chester, PA, 19022-2000, transunion.com/credit-freeze

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the three national credit reporting agencies listed above.

The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day, and year); current address and previous addresses for the past 5 years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state, or military ID card, and a copy of a utility bill, bank, or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

For residents of the District of Columbia: You may also contact the District of Columbia Office of the Attorney General: Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001, (202) 442-9828, <https://oag.dc.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, www.oag.state.md.us.

For residents of Massachusetts: If you are a Massachusetts resident, you also have a right to request a police report about this incident.

For residents of Oregon: You may also contact the Oregon Office of the Attorney General: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, 1-877-877-9392, help@oregonconsumer.gov, www.doj.state.or.us.