



Notice of Data Security Incident

Timber Creek has become aware of a data security incident that may have impacted personal information belonging to certain employees. On April 15, 2021, Timber Creek notified potentially impacted individuals of this incident by letter and provided resources to assist them. The letters include information about this incident and about steps that potentially impacted individuals can take to monitor and help protect their information. Contact information for some potentially affected individuals was not identified and Timber Creek is providing this website posting as substitute notice to those individuals.

On September 13, 2020, Timber Creek discovered that some of our systems had been encrypted. Our immediate concern was to contain the incident and secure our network systems. To that end, we engaged a digital forensics firm to investigate the cause and scope of the incident and determine if any information stored within our systems had been affected. The forensic investigation determined that an unauthorized individual may have had access to certain files on our network. We then conducted a detailed and comprehensive review of the impacted information which concluded on February 10, 2021. The review determined that certain personal information was involved in the incident. We immediately worked to obtain addresses for the impacted individuals. We are not aware of any person's information having been misused.

The digital environment at Timber Creek has been improved to prevent a similar incident from happening in the future. The affected personal information may have included names, Social Security numbers, financial account numbers, and driver's license numbers of current or former employees.

We encourage individuals believed to have been impacted by the incident to carefully review and monitor their various account statements. If you believe that your information has been used to open a new account or to make unauthorized charges, transactions, or withdrawals, you should immediately contact your bank or the relevant account administrator. Timber Creek has established a toll-free call center to answer questions about the incident and related concerns. The call center is available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time and can be reached at 1-800-939-4170. In addition, out of an abundance of caution, Timber Creek is offering identity protection services through IDX to some potentially impacted individuals at no cost..

The privacy and protection of customer information is essential for us. We deeply regret any inconvenience or concern this incident may cause.

We are also providing the following information to help those wanting to know more about steps they can take to protect themselves:

What steps can I take to protect my personal information?

- If you detect any suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should

also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.

- Obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To do so, free of charge once every 12 months, please visit ***.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed below.
- Please notify your financial institution immediately of any unauthorized transactions made or new accounts opened in your name.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identity theft. The FTC's website offers helpful information at ***.ftc.gov/idtheft.
- Additional information on what you can do to better protect yourself is included in your notification below.

What should I do to protect myself from payment card/credit card fraud?

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. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

How do I obtain a copy of my credit report?

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting ***.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
***.transunion.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
***.experian.com

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-888-548-7878
***.equifax.com

How do I put a fraud alert on my account?

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at ***.annualcreditreport.com.

How do I get a Personal Identification Number from the IRS to prevent misuse of my Social Security number in relation to my tax return?

Under certain circumstances, the IRS will provide taxpayers a unique Person Identification Number (“PIN”) to protect victims of identity theft. The IP PIN is a six-digit number assigned to eligible taxpayers to help prevent the misuse of their Social Security number on fraudulent federal income tax returns. A PIN helps the IRS verify a taxpayer’s identity and accept their electronic or paper tax return. When you have an PIN, it prevents someone else from filing a tax return with your SSN. The instructions for getting a PIN are here:

[*****.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin](https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin)

How do I put a security freeze on my credit reports?

Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources:

You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave,
NW
Washington, DC 20580
consumer.ftc.gov, and
***.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

North Carolina Attorney General

9001 Mail Service
Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
*****.riag.ri.gov
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA):

These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit [*****files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf](https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf).