



RECEIVED

MAY 12 2020

CONSUMER PROTECTION

April 30, 2020

Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

Re: Data Breach Notification

Dear Sir:

TD Bank, N.A. is notifying your office of a privacy event impacting New Hampshire residents. Our investigation identified 24 of our customers who are residents of New Hampshire and may have been affected by this incident.

During the pendency of Customer bankruptcies, TD filed documents with the Bankruptcy Court which were not properly redacted of various personally identifiable information (PII). This information would only be available to those who had a subscription to the bankruptcy court electronic filing system. The personal information that may not have been properly redacted on a bankruptcy court filing included name, address, phone number, date of birth, social security number, and/or account number.

TD Bank has notified the affected customers in writing and offered two years of free credit monitoring. A copy of our customer notification letter is enclosed for your reference. Also, TD Bank reviewed every filing it made with respect to the impacted Customer's bankruptcy. If PII was identified, TD Bank filed a motion with the applicable Bankruptcy Court to redact the unredacted PII. Filing of the motion immediately restricted public access to the identified document(s), and those documents will be redacted or replaced with a redacted substitute document. The PII is no longer viewable on the bankruptcy court electronic filing system.

If you need any further information, please contact: N. Patrice Brusko, Chief Privacy Officer, TD Bank, N.A., 9000 Atrium Way, Mount Laurel, NJ 08054 or Patrice.brusko@td.com. Thank you for your attention to this matter.

Sincerely,

N. Patrice Brusko
SVP, Chief Privacy Officer
TD Bank, N.A.

Notice of Data Breach

[Date]

[Name]

[Address]

[Address]

Dear [First Name]

We value your privacy and make every effort to keep your personal information safe. Unfortunately, we're writing today to let you know about a recent incident regarding your personal information.

What Happened?

During the pendency of your bankruptcy, TD filed documents with the Bankruptcy Court which were not properly redacted of various personally identifiable information (PII). This information would only be available to those who had a subscription to the bankruptcy court electronic filing system. We realize this is not news you want to hear, and we're truly sorry. Safeguarding your personal information is something we take very seriously.

What Information Was Involved?

The personal information that may not have been properly redacted on a bankruptcy court filing included your name, address, phone number, date of birth, social security number, and/or account number.

What We Are Doing?

TD reviewed every filing it made with respect to your bankruptcy. If PII was identified, TD filed a motion with the applicable Bankruptcy Court to redact the unredacted PII. Filing of the motion immediately restricted public access to the identified document(s), and those documents will be redacted or replaced with a redacted substitute document. Your PII is no longer viewable on the bankruptcy court electronic filing system.

We Are Offering You Additional Safeguards

We're paying for you to take advantage of a complimentary two-year membership to Fraud-Defender, provided by Merchants Information Solutions. This best-in-class service helps detect misuse of your personal information. It also provides you with identity research and resolution services to protect your identity should you suspect a problem for any reason. Details are included on page 3.

What You Can Do?

Here's what you can do to protect yourself from identity theft and fraud:

Additional information about credit reports and ways to prevent identity theft and fraud is available through the FTC at <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>, by visiting annualcreditreport.com, or by calling 1-877-322-8228.

- **Remain vigilant** for incidents of fraud, identity theft, and errors by regularly reviewing your account statements for any unauthorized activity and monitoring free credit reports over the next twelve to twenty-four months.
- **Establish a password** on your account(s). Also, routinely change online account passwords and security questions here at TD Bank and other companies.
- **Report any suspicious or unauthorized activity** to law enforcement and to the Federal Trade Commission (FTC) at 1-877-FTC-HELP (1-877-382-4357).

- **Notify us immediately** of any suspicious activity or suspected identity theft at 1-800-893-8554.
- **Carefully monitor your 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. You may also have information relating to fraudulent transactions deleted from your credit report.
- **Place a free fraud alert or security freeze on your credit file,** which tells creditors to contact you before they open any new accounts or change your existing accounts – and alerts them of possible fraudulent activity. Fraud alerts last 90 days unless you manually renew them or use an automatic fraud alert feature. You can contact the credit reporting agencies directly at:

Equifax 1-800-525-6285 P.O. Box 740241 Atlanta, GA 30374-0241 https://www.equifax.com/personal	Experian 1-888-397-3742 P.O. Box 2104 Allen, TX 75013-0949 https://www.experian.com	TransUnion Corp 1-800-888-4213 P.O. Box 2000 Chester, PA 19016 https://www.transunion.com
--	---	---

Additional information about credit reports and ways to prevent identity theft and fraud is available through the FTC at <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>, by visiting annualcreditreport.com, by calling **1-877-322-8228**, or by mail to: Federal Trade Commission Consumer Response, 600 Pennsylvania Avenue, Washington, DC 20580.

For More Information

If you have any questions, please call us anytime at [phone number]. Again, we apologize for any concern or inconvenience this may cause. We're committed to delivering a legendary customer experience and truly appreciate the opportunity to regain your trust. Thank you for your patience and understanding.

Sincerely,

[Collections Exec Signature]

Your complimentary two-year Fraud-Defender membership includes:

- Continuous monitoring of your TransUnion credit file with a daily alert of any changes or new items added to your credit file.
- Internet monitoring with daily alerts if we find your personal information exposed in high risk areas of the Internet, including black market and social networking sites. You may register up to 50 unique pieces of personal and account information for monitoring.
- An assigned, professional Identity Theft Recovery Advocate to manage any problems you may have in the future and to work on your behalf to resolve any issues of fraud, if needed.

Complete instructions for activating your free services:

1. Visit tdbank.merchantsinfo.com and click on the red button which reads "Sign up takes 3 minutes with Instant Protection"
2. Next, click on the blue "Enroll" button.
3. Enter this complimentary enrollment code in the field labeled "Certificate Code":
[Code]
4. Follow the instructions on each page to complete your enrollment and identity authentication.
5. For help with enrollment or questions about this product, please call Merchants Information Solutions at **1-800-366-6573**. Normal business hours are Monday – Friday 8:00 AM EST to 8:00 PM EST.

Please take advantage of this complimentary offer by **[Date].**

FEDERAL FAIR CREDIT REPORTING ACT RIGHTS:

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how credit reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of credit reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; credit reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; credit reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

IF YOU ARE A NORTH CAROLINA RESIDENT:

You may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
<http://www.ncdoj.gov>

IF YOU ARE A NEW YORK RESIDENT:

For more information on identity theft, you can visit the following websites:

New York Department of State Division of Consumer Protection: <http://www.dos.ny.gov/consumerprotection>
NYS Attorney General at: <http://www.ag.ny.gov/home.html>

IF YOU ARE A MASSACHUSETTS RESIDENT:

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
<https://www.equifax.com/personal/credit-report-services/>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
<https://www.experian.com/freeze/center.html>

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
<https://www.transunion.com/credit-freeze>

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.