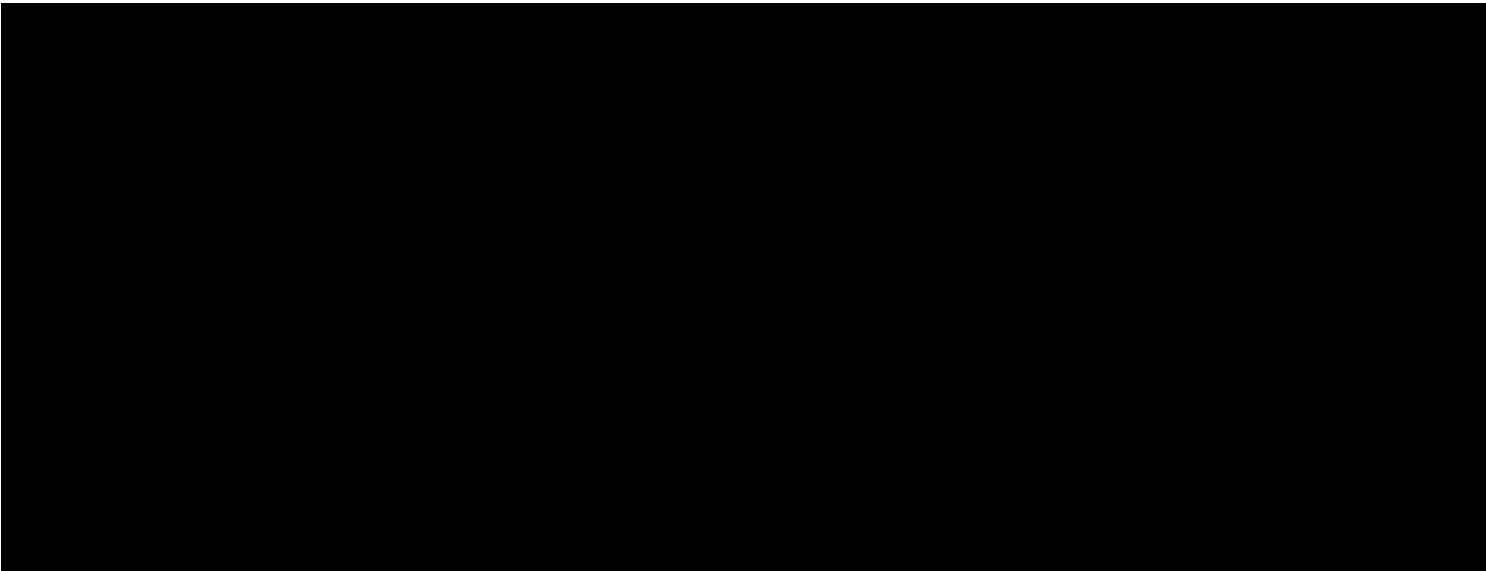




Via Email (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann., Com. Law § 14-3504, I am writing on behalf of Verizon to notify you regarding the nature and circumstances of a recent information security issue. In early April, Verizon was notified by a partner that a partner employee obtained Social Security numbers of Verizon customers and stored these numbers on the partner employee's hard drive. The partner told Verizon that their investigation did not find a reason for the partner's employee to be using this information. The partner terminated this employee and deleted this information.

Verizon is not aware of how the partner employee's obtained customers' Social Security numbers. Verizon has arranged to provide affected individuals with two years of credit monitoring and identity protection services at no cost to them.

Verizon is notifying one Maryland resident whose personal information was affected by this issue. Enclosed for your reference is a copy of the notice being sent to the affected individuals.

Very truly yours,

Stephen Jenkins

Enclosure

Stephen

verizon✓

T. Stephen Jenkins

Managing Associate General Counsel
Privacy & Security Legal

O 202 515 2513
M 908 208 8104
1300 I Street NW
Washington, DC 20005

[Date]

[First Name] [Last Name]

[Street address]

[City, State Zip]

Subject: Important notice

Account number: xxxxxxxxx[NNNN]

Dear [First Name] [Last Name]:

Verizon works hard to protect our customers' accounts. We are writing to let you know about an incident impacting your personal information.

What Happened?

We were alerted by a Verizon partner that the partner's employee improperly accessed your Social Security number for unknown purposes. This person no longer has access to your information.

What Information Was Involved?

We believe the Verizon partner employee had access to your information in your Verizon account and Social Security number.

What We Are Doing?

We investigated the incident. We worked with the Verizon partner to take steps to help ensure that the Verizon partner employee no longer has access to your account.

What You Can Do?

Credit Monitoring

As part of our efforts to assist you, we have retained Experian, a specialist in identity theft protection, to provide you with two years of credit monitoring and identity theft services, free of charge. You can enroll in the program by following the directions below.

- Ensure that you **enroll by:** [Date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website (<https://www.experianidworks.com/3bplus>) to enroll. If you have any questions, you can contact Experian at this toll-free number 877.890.9332
- Provide the following **activation code:** [Code]
- Remember your **engagement number:** [Number]

Please keep this letter; you will need the personal activation code it contains in order to register for services.

More Information

We value the trust our customers place in us, and we regret any inconvenience this incident may have caused you. If you have questions or concerns, please call 1-877-350-7901 for assistance.

Sincerely,

Verizon

Additional Information

Remain Vigilant

We recommend that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as the major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are reported timely.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement authorities, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
<https://www.identitytheft.gov/>

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently, and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide consumer reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at <https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies (Equifax, Experian, and TransUnion) to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you can obtain information from the FTC and the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays in your file for seven years. To place either of these alerts, a consumer

reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide consumer reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. Please be aware, however, 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. The consumer reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each consumer reporting company.

You may contact the nationwide consumer reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
(800) 525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(800) 680-7289
www.transunion.com