



«HM_ENTITY_2»
«HM_ADDRESS_1»
«HM_CITY», «HM_STATE» «HM_ZIP»

August 23, 2021

«EMP_SALUTATION». «EMP_F_NAME» «EMP_L_NAME»
«EMP_ADDRESS_1» «EMP_APT»
«EMP_CITY», «EMP_STATE» «EMP_ZIP»

Dear «EMP_SALUTATION». «EMP_L_NAME»:

On behalf of «HM_ENTITY_2», I am writing to advise you of an ongoing investigation related to a recent security incident that may have affected the personal information stored in files for you. To the best of our knowledge, we are not aware of any actual or attempted misuse of anyone's personal information. However, out of an abundance of caution, we want to make sure that everyone has access to resources that can be used to protect their personal information.

What Happened?

On July 18, 2021, encrypted files were discovered on several systems within the computer network. To the best of our knowledge, local business locations, including operating retail stores, were not affected and normal day to day business operations are being conducted without interruption. Furthermore, the "cloud applications" were not affected either.

What Is Being Done?

This matter has been reported to the federal law enforcement. In addition, cybersecurity professionals have been engaged to investigate what happened and at the same time to further strengthen the security of all systems within the computer network.

What Information Was Available?

An investigation is ongoing to determine which information may have been involved. Since it is possible that «HM_ENTITY_2's corporate file server containing personal identifying information (including names, birth dates and social security numbers) may have been accessed, you are being notified through this letter.

What You Can Do

In order to ensure that all «HM_ENTITY_2» employees have the right resources at their disposal to protect themselves, a two-year credit monitoring and identity protection service from Experian has been purchased for you. This service is at no charge to you. To enroll, please follow the instructions included with this letter.

An Identity Protection Reference Guide which includes additional resources on how to prevent identity theft is included with this letter and we strongly would encourage you to review this information. It offers some helpful tips on how to monitor the use of your personal information.

Please know that we are working very hard to address this situation. We would also ask that you refrain from talking about this matter with anyone outside of the company. We are sorry for any inconvenience this may cause you, and thank you for your support and understanding. If you have any questions, please reach out to our dedicated assistance team at [insert call center number], [insert call center days and times].

Sincerely,

«HM_F_NAME» «HM_L_NAME», «HM_TITLE»

IDENTITY PROTECTION REFERENCE GUIDE

1. Review your Credit Reports. We recommend that you remain vigilant by monitoring your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

2. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax Fraud Reporting
1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000

www.equifax.com

www.experian.com

www.transunion.com

It is only necessary to contact one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your Social Security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

4. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements, medical provider statements, and insurance statements for fraudulent activity and report anything suspicious to the respective institution or provider.

5. You can obtain additional information about the steps you can take to avoid identity theft and more information about fraud alerts and security freezes from the Federal Trade Commission (FTC). You may

contact the FTC, Consumer Response Center at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

District of Columbia Residents: You can obtain additional information about identity theft prevention and protection from the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, <https://oag.dc.gov>.

Iowa Residents: You can report suspected identity theft to law enforcement, the FTC, or to the Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-888-777-4590, <https://www.iowaattorneygeneral.gov/>.

Maryland Residents: You can obtain additional information about identity theft prevention and protection from the Maryland Attorney General, Identity Theft Unit at: 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, 1-888-743-0023 or (410) 576-6491, <https://www.marylandattorneygeneral.gov>.

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, <https://www.mass.gov/service-details/identity-theft>.

New York Residents: You can obtain additional information about identity theft prevention and protection from the New York State Attorney General, The Capitol, State Street and Washington Avenue, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/>.

North Carolina Residents: You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, <https://ncdoj.gov/>.

DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

We are offering you a two-year, complimentary membership for IdentityWorksSM, a product offered by Experian®, to help with detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: [DATE] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [WEBSITE]
- Provide your **activation code**: [INSERT CODE]

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [INSERT] by [DATE]. Be prepared to provide engagement number [INSERT] as proof of eligibility for the identity restoration services by Experian.

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [INSERT]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.