

Attachment

Peabody & Arnold is a law firm headquartered in Boston, Massachusetts with two other offices in New York and Rhode Island. Peabody & Arnold completed an investigation involving suspicious activity originating from one employee's email account. Upon discovery of the incident, Peabody & Arnold secured the employee's email account and launched an investigation to determine the nature and scope of the incident. A cybersecurity firm was engaged to assist in a full forensic analysis of the incident. The investigation determined that an unauthorized person accessed the employee's email account at various times between May 21, 2020 and May 27, 2020. The investigation did not determine whether the unauthorized individual actually viewed or accessed any of the emails in the account; however, Peabody & Arnold was not able to rule out that possibility. Peabody & Arnold searched the contents of the account to identify individuals whose information may have been accessible to the unauthorized individual. On November 12, 2020, Peabody & Arnold determined that an email or attachment in the account contained information pertaining to three Maine residents including the individuals' names and one or more of the following: Social Security number, driver's license number and/or financial account number.

Beginning today, December 21, 2020, Peabody & Arnold will mail written notification via First-Class U.S. mail to the Maine residents.¹ A sample copy of the notification letter is enclosed. Peabody & Arnold has offered the Maine residents whose Social Security numbers and/or driver's license numbers were involved a complimentary, one-year membership in credit monitoring and identity protection services through Experian. Peabody & Arnold has established a dedicated phone number that individuals may call with related questions.

To further protect personal information, Peabody & Arnold is taking steps to enhance its existing security protocols and re-educating staff for awareness on these types of incidents. Peabody & Arnold has enabled two-factor authentication on an enterprise-wide level, reset passwords for all users in its email environment, and configured its email tenant to disable legacy email protocols.

¹ This notice does not waive Peabody & Arnold's objection that Maine lacks personal jurisdiction over it regarding any claims related to this incident.

[REDACTED]
[REDACTED]
[REDACTED]

C-62

December 17, 2020

Dear [REDACTED]:

At Peabody & Arnold LLP, we understand the importance of protecting and securing the personal information that we maintain. I am writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

We completed an investigation into suspicious activity originating from one Peabody & Arnold employee's email account. As soon as we became aware of the activity, we immediately took measures to secure the email account and launched an internal investigation. A cybersecurity firm was engaged to assist in a forensic analysis of this incident. The investigation determined that an unauthorized person accessed the employee's email account at various dates between May 21, 2020 and May 27, 2020.

The investigation did not determine whether any specific emails or attachments were viewed by the unauthorized person; however, we were not able to rule out that possibility. In an abundance of caution, we searched the full contents of the account to identify individuals whose information may have been accessible to the unauthorized person. On November 12, 2020, we determined that an email or attachment in the account contained your name and Social Security number.

While we have no indication that your information was actually viewed by the unauthorized person or that it has been or will be misused, we wanted to notify you of this incident and assure you that we take it very seriously. We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. As an added precaution, we are also offering you a complimentary one-year membership with Experian's® IdentityWorksSM. This product helps detect possible misuse of your personal information and provides you with identity protection support. **For more information on IdentityWorksSM, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take, please see the additional information provided in this letter.** For more information on identity theft prevention and your complimentary one-year membership, please see the additional information provided in this letter.

Your confidence and trust are important to us, and we sincerely regret any concern or inconvenience this incident may cause. To further protect personal information, we are taking steps to enhance our existing security protocols and re-educating our staff for awareness on these types of incidents. If you have any questions, please call 1-800-295-9470, Monday through Friday from 8:00 A.M. through 5:00 P.M. Eastern Time.

Sincerely,



Robert McCall
Managing Partner

Activate IdentityWorks Credit 3B Now in Three Easy Steps

To activate your membership and start monitoring your personal information please follow the steps below:

1. ENROLL by: **March 7, 2021** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: [REDACTED]

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 **877.288.8057** by **March 7, 2021**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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, Equifax and Transunion files for indicators of fraud.
- **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.
- **\$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 877.288.8057. 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 one year 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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If your health insurance or medical information was involved, it is also advisable to review the billing statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact the insurer or provider immediately.

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts 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 one year. 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 seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.