

Appendix

On March 4, 2024, Tri Delta identified and addressed a phishing incident in which a document containing employee 2023 W2 statements was inadvertently emailed to an unauthorized person that same day. Upon learning of the incident, Tri Delta immediately took steps to identify the information that was contained in the document and notified individuals of the incident via email. Tri Delta also notified the IRS and subsequently notified law enforcement. The information sent to the unauthorized person contained the name and Social Security number of one Maine resident.

On April 1, 2024, Tri Delta mailed a notification letter via First Class mail to the Maine resident in accordance with Me. Rev. Stat. Tit. 10, §1348. A copy of the notification letter is attached. Tri Delta is offering the resident a complimentary, two-year membership to credit monitoring and identity theft protection services. Tri Delta has also provided individuals with a number they can call to obtain more information regarding the incident.

To help prevent something like this from happening again, Tri Delta has provided additional training to employees on how to identify and avoid phishing emails.



«First_Name» «Last_Name»
«Primary_Address_Line_1» «Primary_Address_Line_2»
«Primary_CityMunicipality», «Primary_StateProvince» «Primary_ZipPostal_Code»

April 1, 2024

Dear «First_Name»:

Tri Delta understands the importance of protecting the information we maintain. We are writing to provide an update to the email notification we sent you on March 4, 2024. This letter explains what happened, measures we have taken, and some steps you may choose to take.

What Happened?

On March 4, 2024, we identified and addressed a phishing incident in which a document containing your 2023 W2 statement was inadvertently emailed to an unauthorized person that same day. Upon learning of the incident, we immediately took steps to identify the information that was contained in the document and notified you of the incident via email. We also notified the IRS and subsequently notified law enforcement.

What Information Was Involved?

The information sent to the unauthorized person was the information contained in your 2023 W2 statement, including your name, address, and Social Security number.

What We Are Doing.

We wanted to notify you of this incident and assure you that we take it seriously. To help prevent something like this from happening again, we have provided additional training to employees on how to identify and avoid phishing emails.

What You Can Do.

We have arranged for you to receive a complimentary two-year membership to Identity Defense credit monitoring service. This product helps detect possible misuse of your information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Identity Defense is completely free to you, and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and Identity Defense, including instructions on how to activate your complimentary two-year membership, as well as some additional steps you can take in response, please review the pages attached to this letter.

You may also choose to obtain an Identity Protection Personal Identification Pin (“IP PIN”) from the Internal Revenue Service. You can obtain a pin online at this link: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

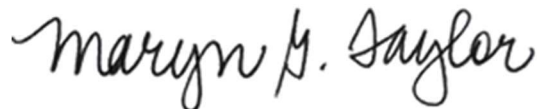
14951 Dallas Parkway, Suite 500 Dallas, TX 75254 817.633.8001 www.tridelta.org

In addition, we encourage you to always be vigilant against the possibility of phishing attempts via email or text message and to verify sources of communication before clicking on links or providing your information.

For More Information.

We regret that this occurred and apologize for any inconvenience. If you have additional questions, please call (817) 633-8001, Monday through Friday, between 8:30 a.m. and 5:00 p.m., Central Time.

Sincerely,

A handwritten signature in black ink that reads "Maryn G. Taylor". The signature is written in a cursive, flowing style.

Maryn G. Taylor
Senior Director of People and Culture



«First_Name» «Last_Name»
Enter your Activation Code: «Code»
Enrollment Deadline: 6/30/2024
Service Term: 24 months

Identity Defense Total

Key Features

- 3-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit «Link»

1. Enter your unique Activation Code «Code»
Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
Enter your email address, create your password, and click 'Create Account'.
3. Register
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is 6/30/2024. After 6/30/2024, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by 6/30/2024, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. 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, 1-888-378-4329
- *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.identitytheft.gov

Fraud Alerts and 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:

- *Equifax Security Freeze*, PO Box 105788, Atlanta, GA 30348, www.equifax.com
- *Experian Security Freeze*, PO Box 9554, Allen, TX 75013, www.experian.com
- *TransUnion Security Freeze*, PO Box 160, Woodlyn, PA 19094, www.transunion.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.

Tri Delta is located at 14951 N. Dallas Pkwy. Suite 500, Dallas, Texas 75254 and can be reached by phone at 817-633-8001.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, <https://www.marylandattorneygeneral.gov/>

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov