



April 24, 2020

Anjali C. Das  
312.821.6164 (direct)  
Anjali.Das@wilsonelser.com

RECEIVED

MAY 01 2020

CONSUMER PROTECTION

Via Postal Mail Only

**Attorney General Gordon J. MacDonald**  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent Trinity Benefit Advisors (“Trinity”), headquartered in Tennessee, with respect to a potential data security incident described in more detail below. Trinity takes the security and privacy of the information in its control very seriously, and has taken steps to help prevent a similar incident from occurring in the future.

**1. Nature of the security incident.**

Trinity is an employee benefits firm that provides benefits services to its corporate clients. On May 6, 2019, Trinity became aware of suspicious activity on an employee’s email account. Thereafter, Trinity engaged with an independent computer forensic company to analyze the nature and extent of the unauthorized access. The forensic investigation determined that a malicious inbox rule caused over 10,000 incoming and outgoing messages to be forwarded to an unknown party. After the completion of the forensics investigation, the forwarded emails were reviewed for content. These forwarded emails contained individuals’ names in combination with Social Security numbers and other employee benefit related information.

Since Trinity did not have addresses for all of the members affected population, Trinity worked closely with its corporate clients over the course of many months to identify the individuals whose personally identifiable information (“PII”) may have been contained within the affected email account that required notification. This included all individuals that had submitted benefit enrollment forms via email during the prior 3-year period. The list of individuals for notification was completed in January 2020.

Thereafter, Trinity reached out to vendors to assist with the notification process. The first vendor that Trinity engaged failed to proceed in a timely manner and declined to utilize the data file template prepared by Trinity for notification purposes. Based on this delay and lack of

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky  
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix • San Diego  
San Francisco • Sarasota • Stamford • Virginia • Washington, DC • West Palm Beach • White Plains

wilsonelser.com



cooperation, Trinity was forced to engage a second vendor for notification on March 30, 2020. The individual notification letters were sent out by the second vendor on April 24, 2020.

**2. Number of New Hampshire residents affected.**

A total of six (6) residents of New Hampshire may have been potentially affected by this incident. A notification letter to this individual was mailed on April 24, 2020 by first class mail. A sample copy of the notification letter is included with this letter.

**3. Steps taken.**

Trinity takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar event from occurring in the future, as well as to protect the privacy and security of potentially impacted individuals' information. This includes, but is not limited to, changing passwords, providing users with increased training on network security, implementing multi-factor authentication, and reporting the incident to government regulators. Trinity is also providing potentially impacted individuals with identify theft protection and credit monitoring services for a period of 12 months, at its own expense, through Kroll.

**4. Contact information.**

Trinity remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at [Anjali.Das@wilsonelser.com](mailto:Anjali.Das@wilsonelser.com) or (312) 821-6164.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**

A handwritten signature in cursive script, appearing to read "Anjali C. Das".

Anjali C. Das

Enclosure.



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

We are writing to inform you of a data security incident involving Trinity Benefit Advisors that may have resulted in unauthorized access to some of your personal information. We take the privacy and protection of your personal information very seriously. We apologize and regret any inconvenience this may cause. This letter contains information about what happened, steps we have taken and resources we are making available to you to help monitor your identity.

Trinity Benefit Advisors works with your employer to provide your employee benefits. In or about May 2019 we discovered that a Trinity employee's email account was accessed by an unauthorized party. Once we discovered evidence suggesting that the email account was accessed by an unauthorized party, we immediately changed the password to the account. We also conducted a thorough investigation with the assistance of computer forensic professionals who confirmed that the unauthorized party did access the employee's account. We have worked with your current or former employer to identify all individuals whose information may have been accessible from within the affected email account.

We determined that your information may have been accessible from within the affected email account. The information that was potentially accessible includes your name and one or more of the following personal attributes: Social Security Number, date of birth, address, and/or medical information, such as information provided during benefits enrollment periods. At this time, we have no evidence that anyone's personal information has been misused as a consequence of this incident.

In an effort to help relieve any concerns you may have, we are providing you with complimentary resources to help monitor your identity, whether or not it was affected. We have secured the services of Kroll to provide identity monitoring services at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

*You have until **July 17, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

We take the security of all information in our systems very seriously and want to assure you that we are taking steps to prevent a similar event from occurring in the future. Those steps include changing passwords, providing users with increased training on network security, implementing multi-factor authentication, and reporting the incident to government regulators.

We sincerely regret any inconvenience that this matter may cause you and remain dedicated to protecting your information. If you have any questions, please call 1-888-921-0511, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your membership number ready.

Sincerely,

A handwritten signature in black ink that appears to read "Drew Mann".

Drew Mann

## Additional Important Information

---

### **For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina:**

It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

---

### **For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:**

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

---

### **For residents of Iowa:**

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

---

### **For residents of Oregon:**

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

---

### **For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:**

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

#### **Maryland Office of the Attorney General**

Consumer Protection  
Division  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

#### **Rhode Island Office of the Attorney General**

Consumer Protection  
150 South Main Street  
Providence RI 02903  
1-401-274-4400  
[www.riag.ri.gov](http://www.riag.ri.gov)

#### **North Carolina Office of the Attorney General**

Consumer Protection  
Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-566-7226  
[www.ncdoj.com](http://www.ncdoj.com)

#### **New York Office of the Attorney General**

Bureau of Consumer  
Frauds & Protection  
The Capitol  
Albany, NY 12224-0341  
1-800-771-7755  
<https://ag.ny.gov/consumer-frauds/identity-theft>

#### **Federal Trade Commission**

Consumer Response Center  
600 Pennsylvania Ave, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

---

### **For residents of Massachusetts:**

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

---

### **For residents of all states:**

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud\\_Alert\\_Request\\_Form.pdf](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf)); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**Security Freeze:** You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

**Equifax Security Freeze**

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

**Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
www.experian.com/freeze  
888-397-3742

**TransUnion (FVAD)**

P.O. Box 2000  
Chester, PA 19022  
freeze.transunion.com  
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.



**TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You've been provided with access to the following services<sup>1</sup> from Kroll:

**Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

**Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.