

ALEXANDER F. KOSKEY, III, CIPP/US, CIPP/E, PCIP
Direct Dial: 404.443.6734
Email: akoskey@bakerdonelson.com

January 3, 2022

VIA EMAIL

Attorney General Brian E. Frosh
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: *TCW, Inc. – Notice of Data Incident*

Dear Attorney General Frosh:

We represent TCW, Inc. (“TCW”), whose principal place of business is located at 22 Stanley Street, Nashville, TN 37210.¹ TCW is a commercial transportation and trucking company.

This correspondence is to notify you of a security incident where some of TCW’s systems became encrypted. Upon identifying the incident, TCW immediately launched an investigation to determine the full scope of the incident and secure its network systems. TCW discovered that there was potentially unauthorized access to personally identifiable information (“PII”) in TCW’s network on or about December 2, 2021. Although there is no evidence that any PII was exfiltrated from TCW’s network, due to the risk that PII may have been accessed during the incident and in abundance of caution, notification letters are being sent via U.S. Mail to 2 residents of your state on or about January 3, 2022. The notification letters include instructions for activating one (1) year of credit monitoring services at no cost to the residents. The PII that was potentially at risk included first and last names, Social Security numbers, and financial account numbers. A sample notification letter is enclosed for your reference and includes:

- A description of the security incident;
- Steps taken to investigate the incident;
- Steps taken to mitigate any potential harm to individuals;
- Instructions for activation of 1 year of free credit monitoring and identity theft protection services;

¹ By providing this notice, TCW does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

January 3, 2022

Page 2

- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this incident.

TCW is fully committed to protecting the confidentiality of personal information. We will follow up this correspondence with any forms or other documents that may need to be completed. Please contact me if you require any additional information regarding this incident.

Best regards,

BAKER, DONELSON, BEARMAN,
CALDWELL & BERKOWITZ, PC



Alexander F. Koskey, III

Exhibit 1: Sample notification letter to 2 residents



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

TCW, Inc. ("TCW") is writing to inform you of a security incident which may have involved some of your personal information. We take the privacy and security of your personal information seriously. This letter contains information about the incident, our response, and certain steps you can take to help safeguard your personal information, should you feel appropriate to do so.

What Happened? On October 27, 2021, TCW discovered that some of our systems had been encrypted. Our immediate concern was to contain the incident and secure our network systems. We immediately commenced an investigation, with the assistance of third-party cybersecurity experts, to determine the full nature and scope of the incident and determine if any information stored within our network had been impacted. Through this investigation, we determined that an unauthorized individual may have had access to certain files within our network between October 26, 2021 and October 27, 2021. On December 2, 2021, following a comprehensive analysis, it was determined that your personal information was potentially involved in the incident. We are not aware of any misuse of your information as a result of this incident.

What Information Was Involved? The information that may have been accessed by the unauthorized individual include your <<DATA ELEMENTS>>.

What We Are Doing. Upon becoming aware of the incident, in addition to the steps described above, we immediately reset all user passwords to block any unauthorized access. We are also taking steps to enhance our data security which includes implementing additional technical safeguards within our network. Although we are not aware of any misuse of your information as a result of this incident, we are offering you access to complimentary credit monitoring services through Equifax. These services will be available for <<CM Length>> months at no cost to you as a valued current or former employee of TCW. This letter includes instructions on how to activate these services. Please note that you must complete the activation process yourself.

What You Can Do. We recommend that you activate the complimentary credit monitoring services we are making available to you. We also encourage you to remain vigilant against incidents of identity theft and fraud and to monitor your credit reports and financial statements for suspicious activity. We also recommend that you review the additional information we are enclosing in this letter about steps you can take to help safeguard your information as you deem appropriate.

For More Information. If you have additional questions about this incident, please call 855-604-1661, toll-free, between 9:00 a.m. and 9:00 p.m., Eastern Time, Monday through Friday (excluding major U.S. holidays).

We remain fully committed to protecting your personal information. We sincerely apologize for any concern or inconvenience this may cause you.

Sincerely,

Ben Banks,
Vice President



Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<Activation Code>> then click “Submit” and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click “Continue”.
If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
 2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
 3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
 4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page.
Click ‘Sign Me Up’ to finish enrolling.
- You’re done!**
The confirmation page shows your completed enrollment.
Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded. ²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com ⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Below are additional actions you may take, if you feel it is necessary.

FREEZE YOUR CREDIT FILE. You have a right to place a ‘security freeze’ on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Note that a security freeze generally does not apply to existing account relationships and when a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a security freeze.

To place a security freeze on your credit report, contact each of the three major consumer reporting agencies using the contact information listed below:

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES

Equifax

P.O. Box 105788
Atlanta, GA 30348
1 - 800-685-1111
www.equifax.com

Experian

P.O. Box 9554
Allen, TX 75013
1 - 888-397-3742
www.experian.com

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com

To request a security freeze, you will need to provide the following:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the freeze.

PLACE FRAUD ALERTS ON YOUR CREDIT FILE. As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is an alert lasting 7 years. Contact the credit reporting agencies listed above to activate an alert.

REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS, & REPORT FRAUD. As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, carefully reviewing your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity. Report suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor and law enforcement. (For Oregon & Iowa residents: Report any suspected identity theft to law enforcement, Federal Trade Commission, and your State Attorney General.)

ORDER YOUR FREE ANNUAL CREDIT REPORTS. Visit www.annualcreditreport.com or call 877-322-8228 to obtain one free copy of your credit report from each of the three major credit reporting bureaus annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

FILE OR OBTAIN A POLICE REPORT. You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report incidents of identity theft to local law enforcement or to the Attorney General.

OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC / STATE ATTORNEY GENERAL.

Go to <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html>. The Federal Trade Commission also provides information at www.ftc.gov/idtheft. The FTC can be reached by phone: 1-877-438-4338; TTY: 1-866-653-4261 or by writing: 600 Pennsylvania Ave., NW, Washington, D.C. 20580. Your State Attorney General also may provide information.

FAIR CREDIT REPORTING ACT: You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit “prescreened” offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Please note that identity theft victims and active duty military personnel may have additional rights under the FCRA.

For residents of North Carolina: The North Carolina Office of the General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, and www.ncdoj.com. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For residents of Maryland: The Maryland Office of the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us. You can obtain information from the Attorney General or Federal Trade Commission about preventing identity theft.

For residents of New Mexico: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Furthermore, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccuracies, incomplete or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

For residents of New York: The Attorney General may be contacted at: Office of Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For residents of Rhode Island: The Rhode Island Office of the Attorney General can be contacted at: 150 South Main Street, Providence, RI 02903, 1-401-274-4400, and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident.

For residents of the District of Columbia: The Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001, by phone at (202) 727-3400; and, <https://oag.dc.gov/>. You may obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.