



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

411 Theodore Fremd, Ste 206S
Rye, NY 10580

October 19, 2023

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Trust Benefit Technologies LLC (“TBT”) located at 2011 E Financial Way #220, Glendora, California 91741, and are writing to notify your office of an incident that may affect the security of certain personal information relating to two (2) New Hampshire residents. By providing this notice, TBT does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 22, 2023, TBT identified suspicious activity within its computer network. In response, it immediately took steps to secure its environment and launched an investigation to determine the nature and scope of incident. TBT’s investigation determined that between May 16, 2023 and May 22, 2023, an unknown, unauthorized actor gained access to certain TBT computer systems and potentially accessed certain files stored on accessed computer systems.

The information that could have been subject to unauthorized access includes

Notice to New Hampshire Residents

On or about October 19, 2023, TBT provided written notice of this incident to two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, TBT moved quickly to investigate and respond to the incident, assess the security of TBT systems, and identify potentially affected individuals. Further, TBT notified federal law enforcement regarding the event. TBT is also working to implement additional safeguards and training to its employees. TBT is providing access to credit monitoring services for through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, TBT is providing impacted individuals with guidance on how to better protect against identity theft and fraud. TBT is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

TBT is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Michele Veltri of
MULLEN COUGHLIN LLC

MTV/jc2
Attachment

EXHIBIT A



October 19, 2023

Notice of Security Incident

Dear 

Trust Benefit Technologies, LLC (“TBT”) writes to inform you of a cyber incident that may impact the privacy of some of your information. While we do not have any indication of any identity theft or fraud occurring as a result of this incident, this notice provides you with additional information about the incident, our response, and steps you can take to further protect your information against identity theft and fraud, should you determine it is appropriate to do so.

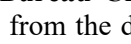
What Happened? On May 22, 2023, TBT identified suspicious activity within our computer network. In response, we immediately took steps to secure our environment and launched an investigation to determine the nature and scope of incident. Our investigation determined that between May 16, 2023 and May 22, 2023, an unknown, unauthorized actor gained access to certain TBT computer systems and potentially accessed certain files stored on accessed computer systems.

What Information Was Involved? TBT began a thorough review of the relevant files to identify individuals with personal information that was potentially impacted. This thorough investigation recently concluded, and on or about June 26, 2023, we determined that your

were potentially accessed by an unknown, unauthorized actor as a result of this incident. Again, at this time, we have received no indication of any identity theft or fraud occurring as a result of this incident.

TBT was in possession of this data in order to prepare benefit administration reports for its client, Pacific Southwest Administrators, pertaining to the Southern California, Arizona, Colorado and Southern Nevada Glaziers, Architectural Metal and Glassworkers Pension Plan (the “Glaziers Pension Plan”). Pacific Southwest Administrators is the third-party administrator for the Glaziers Pension Plan.

What We Are Doing. TBT takes this incident and the security of information within our care very seriously. Upon discovery of this incident, we immediately launched an in-depth investigation to determine the full nature and scope of this incident and moved quickly to assess the security of our systems and notify potentially affected individuals. As part of our ongoing commitment to the privacy of information in our care, we are working to implement additional security measures to further protect against similar incidents in the future. We also notified federal law enforcement of this event. We will notify state regulators, as required.

As an added precaution, we would like to offer you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for  from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout

through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. If you wish to receive these services, you should follow the below enrollment instructions as we are unable to activate these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your accounts statements and credit reports to detect errors or suspicious activity. You can find more information about obtaining a free copy of your credit report, protecting against potential identity theft and fraud, and other resources available to you in the enclosed *Steps You Can Take to Help Protect Your Information*. You may also enroll in the complimentary credit monitoring services available to you; detailed instructions for enrolling in these services are enclosed.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to

1

Sincerely,

Bruce Biller
President
Trust Benefit Technologies
2011 East Financial Way | Suite 220
Glendora, CA 91741

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/TBT> and follow the instructions provided. When prompted please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.