



Jena M. Valdetero
Tel 312.456.1025
jena.valdetero@gtlaw.com

April 10, 2023

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notification of Security Incident

Dear Attorney General Frosh:

We are writing to inform you that our client, Trafera, LLC, which operates the ecommerce website www.shop.trafera.com ("Trafera"), is notifying approximately three individuals who reside in Maryland of a data security incident that may have impacted some of their personal information.

On March 10, 2023, Trafera discovered that customer usernames and passwords may have been acquired by an unauthorized third party from its computer network on February 22, 2023, as determined by internal and external forensic investigations. These usernames and passwords, if used, could have provided access to customer account information, including name, address, email, and phone number. We do **not** store credit card or other payment information on that platform, as a result, **credit card information was not at risk**.

We take the security and privacy of our customers very seriously and have immediately disabled service on that platform out of an abundance of caution. We are in the process of migrating to a new e-commerce platform and will focus all e-commerce efforts onto the new platform. We have also advised our customers to take precautionary measures, such as changing their passwords and monitoring their accounts for any suspicious activity

Trafera provided notice on April 1, 2023. An example of the notification is attached.

Please contact me for any additional information. Thank you.

April 10, 2023

Page 2

Very truly yours,

Jena M. Valdetero
Shareholder



@ Trafera.com
2550 University Ave W
Ste 315-S
Saint Paul, MN 55114
(888) 862-5120

Dear Valued Customer,

On March 10, 2023, we identified unauthorized access to some data on an e-commerce platform we have used at shop.trafera.com, and it is possible the following information was accessed by unknown entities:

- Username (email)
- Password
- Name
- Address
- Phone

We do **not** store credit card, Social Security information or other payment information on that platform. The platform does not maintain any connections to any of our other systems, and there is no evidence any other data has been accessed.

We believe the earliest date of access was February 22, 2022.

We take the security and privacy of our customers very seriously. We contracted with a cyber security firm to identify the extent of potential access, and have decided to immediately discontinue use of our current e-commerce platform out of an abundance of caution. We are already in the process of migrating to a new e-commerce platform, so shop.trafera.com will remain closed until new infrastructure is in place. In the meantime, please contact us via phone or e-mail for any of your educational technology needs.

We advise you to take precautionary measures such as changing your passwords especially if you utilize the same user credentials and password on other online accounts and monitoring your accounts for any suspicious activity. More information about how you can protect yourself is on the reverse side of this letter.

We apologize for any inconvenience this incident may have caused and assure you that we are doing everything we can to safeguard all data entrusted to us.

If you have any questions or concerns, please do not hesitate to contact us at support@trafera.com or at 888-862-5120.

Sincerely,

Trafera

Important Additional Information

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

Massachusetts and Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

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

You can obtain information from the Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. There was 1 Rhode Island resident notified in this incident.

Federal Trade Commission,	Maryland Office of Attorney General	New York Attorney General	North Carolina Attorney General	Rhode Island Office of Attorney General
600 Pennsylvania Ave, NW Washington, DC 20580	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226	150 South Main St Providence RI 02903 1-401-274-4400
1-877-IDTHEFT (438-4338) www.identitytheft.gov	www.oag.state.md.us	www.ag.ny.gov	www.ncdoj.com	www.riag.ri.gov

For residents of all states:

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, 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 www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

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), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). 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. 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 for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports 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 by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.experian.com/freeze/center.html
1-800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016-2000
www.transunion.com/credit-freeze
1-800-680-7289