401 9th Street, N.W.
Suite 1000
Washington, D.C. 20004

troutman pepper

Kim Phan
Kim.Phan@troutman.com

December 21, 2022

VIA ELECTRONIC MAIL AND OVERNIGHT MAIL DELIVERY

Maryland Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

I am writing on behalf of my client, Tally Technologies, Inc. (Tally), about a recent data security incident. Tally is a California-based financial services technology company engaged primarily in consumer lending. This incident potentially impacted one (1) state resident. Notice of the incident will be sent via email on or about December 21, 2022 to this Tally customer. We have provided you with a sample consumer notice with this letter.

On November 27, 2022, we detected a high volume of suspicious login attempts. We immediately took steps to secure our digital environment and launched an investigation into such activity. We believe that an unauthorized party acquired customer credentials, such as usernames, from an unrelated source and attempted to use such credentials to access Tally accounts. We have no reason to believe that our customers' credentials were acquired through any type of breach or hack of Tally systems.

The following information may have been compromised if the unauthorized party was able to access a customer's account:

- Tally account information, such as name, birthdate, email address, phone, mailing address, reported annual income, credit line, balance, and recent payment information.
- Credit card information, if any card is currently linked by the customer to the Tally account, such as the name of the credit card companies relevant to the customer's loan account, the last four digits of the customer's credit card account number, the APR rate for the credit card, the credit card payment due date, balance, and the history of prior credit card payments made using the customer's Tally line of credit.
- Payment information, such as the customer's checking account information, if a bank account is currently linked by the customer to the Tally account, which in this instance is limited to the customer's bank's name, the customer's account

401 9th Street, N.W.
Suite 1000
Washington, D.C. 20004

troutman pepper

Kim Phan
Kim.Phan@troutman.com

name, the last four digits of the customer's account number, and the customer's checking account balance.

For this Maryland customer, no credit card or payment account information is currently linked to the customer's Tally account, so this information was not compromised.

We have required this potentially affected customer to reset the customer's password. We are implementing additional technical security measures to prevent future incidents. Additionally, we are offering the customer complimentary identity protection services.

Should you have any questions or concerns about this matter, please do not hesitate to contact me using the contact information provided below.

Sincerely,

Kim Phan
Direct: 202.274.2992
kim.phan@troutman.com

Tally Technologies, Inc.
P.O. Box 411165
San Francisco, CA 94141

December 21, 2022

Dear <<First Name>>:

We are writing to inform you of a recent data security incident we experienced that may impact your personal information. This letter includes a description of this incident, as well as information about steps you can take to protect your information.

What Happened: On November 27, 2022, we detected a high volume of suspicious login attempts. We immediately took steps to secure our digital environment and launched an investigation into such activity. We believe that an unauthorized party acquired customer credentials, such as usernames and passwords, from an unrelated source and attempted to use such credentials to access Tally accounts. We have no reason to believe that our customers' credentials were acquired through any type of breach or hack of Tally systems, but rather through a third party.

What Information Was Involved: The following information may have been compromised if the unauthorized party was able to access a Tally account:

- Tally account information, such as your name, birthdate, email address, phone, mailing address, reported annual income, and if applicable, credit line, balance, and recent payment information.

- Credit card information, if you currently have any card linked to your Tally account, such as the name of the credit card companies relevant to your loan account, the last four digits of your credit card account number, the APR rate for your credit card, your credit card payment due date, balance, and the history of prior credit card payments made using your Tally line of credit.

- Payment information, such as your checking account information, if you currently have any bank account linked to your Tally account, which in this instance is limited to your bank's name, your account name, the last four digits of your account number, and your checking account balance.

However, please be aware that you have not added any credit card or payment information to your Tally account, so this information was not compromised.

We have no indication that any of your information has actually been misused.

What We Are Doing: We have required any potentially affected customers to reset their Tally passwords. If you use the same username and password for other, non-Tally online accounts, you should change your password on those accounts as well. We are also implementing additional technical security measures to prevent future incidents. We are also providing you with information about steps that you can take to help protect your personal information, including offering you complimentary identity protection services – enrollment information appears below in this letter.

What You Can Do: While we have received no indication that you information has been misused; we advise you to remain vigilant for signs of unauthorized activity by reviewing your credit reports and financial statements. For more information on how you can protect your personal information, please review the resources provided on the following pages.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-866-508-2559 (Monday through Friday between 8 a.m. to 5 p.m. PT) or email support@meettally.com. You can also contact us via mail at this address: P.O. Box 411165, San Francisco, CA 94141.

tally

The security of your information is a top priority for us. We take your trust in us and this matter very seriously, and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Tally Technologies, Inc.

Additional Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report (e.g., by filing a police report) any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Military members may also place an Active-Duty Military Fraud Alert on their credit reports while deployed. An Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

How do I place a freeze on my credit reports? You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact each of the credit reporting agencies identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

How do I lift a freeze from my credit reports? 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 via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

Additional Information for Maryland residents: You can obtain information from the Maryland Office of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take to prevent identity theft.

- You may contact and obtain information from your state attorney general at: 200 Saint Paul St, Baltimore, MD 21202; (410) 576-6350; www.marylandattorneygeneral.gov.
- Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580; http://www.consumer.gov/idtheft; 1-877-IDTHEFT (438-4338), TTY: (866) 653-4261.

tally

EQUIFAX®

<FIRST NAME> <LAST NAME>
Enter your Activation Code: *<ACTIVATION CODE>*
Enrollment Deadline: *<DEADLINE MMMM DD, YYYY>*

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 notifications[1] 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 alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- 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 theft[4]

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.

[1]WebScan 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. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking 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 [4]The 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.