uphold

28078

[Date]
Uphold HQ Inc.
530 Fifth Ave., Ste. 3A,
New York,
NY 10036

Notice of Data Breach

Dear [NAME]:

We're writing to inform you of a recent security incident at our card processor that involved the disclosure of your personal information.

Your trust and safety remains our highest priority and we'd like to explain what happened, how we handled the situation, and how we can work together to defeat such incidents in the future.

WHAT HAPPENED?

On June 11, 2022, a third-party maliciously misused privileged credentials to gain access to your account information held at our card processor. After becoming aware of the incident, we and our card processor took steps to immediately restrict further access to your information.

We launched a forensic investigation and determined that the unauthorized person accessed and downloaded data from a server containing limited personal information that you provided us for purposes of servicing your cardholder account.

WHAT INFORMATION WAS INVOLVED?

The types of personal information that the unauthorized third-party may have obtained included your name, address, phone number, email address, a reissued debit card number, and a one-time-passcode that can be used to link that debit card to a digital wallet. Please note that your date of birth and social security number were not accessed, and your Uphold login credentials remain secure.

WHAT WE ARE DOING?

We've completed a detailed review of the incident and the population of affected individuals.

Our card processor has implemented the additional security controls and processes to eliminate identified weaknesses to prevent this type of incident from happening again.

If you have requested one, we've also issued you with a new replacement debit card. If you have not done so yet and wish to request a new replacement debit card, please contact us at cardsupport@uphold.com.

Lastly, we've refunded you for transactions that you reported to us as unauthorized and any other transactions that we believe may have been unauthorized. If you identify other transactions that were not properly authorized by you, please contact us immediately at cardsupport@uphold.com.

WHAT YOU CAN DO?

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly contact our support team by email cardsupport@uphold.com for immediate assistance.

To temporarily freeze your Uphold account at any time, please follow the steps outlined here.

If you would like to take additional steps to protect your personal information, we've attached helpful resources on how to do so, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file where relevant.

FOR MORE INFORMATION

We take our responsibility to protect your information extremely seriously, and sincerely regret any inconvenience this incident has caused you.

If you have any questions, you can contact us by email at cardsupport@uphold.com or call 1-855-568-8580.

Chris Ampofo
Chief Information Officer

ADDITIONAL RESOURCES

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity:

As a precautionary measure, it is recommended that you remain vigilant by reviewing your credit reports and account statements 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 any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. You can contact the FTC at:

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

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 https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at http://www.annualcreditreport.com/manualRequestForm.action Credit reporting agency contact details are provided below.

- Equifax:
    - equifax.com equifax.com/personal/credit- report-services
    - P.O. Box 740241 Atlanta, GA 30374
    - 866-349-5191
- Experian:

- experian.com experian.com/help
  - P.O. Box 2002 Allen, TX 75013
  - 888-397-3742
- TransUnion:
  - transunion.com transunion.com/credit-help
  - P.O. Box 1000 Chester, PA 19016
  - 888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert:

You may want to consider placing a fraud alert on your credit file. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays 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.

Security Freeze:

You have the ability to place a security freeze on your credit report at no charge. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent but may delay your ability to obtain credit. To place a security freeze, you must contact each of the three credit bureaus listed above and may be required to provide your full name; SSN; date of birth; the addresses where you have lived over the past five years; proof of current address, such as a utility bill or telephone bill; a copy of a government issued identification card; and if you are the victim of identity theft, the police report, investigative report, or complaint to a law enforcement agency.

- The credit reporting agencies 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 remove the security freeze, you must contact each of the three credit bureaus 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 your request to remove the security freeze.

Federal Fair Credit Reporting Act Rights:

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, 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 reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information:

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado, Delaware, and Illinois residents: You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566- 7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

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

For Georgia, Maryland, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For New York residents: You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, http://www.ag.ny.gov/home.html, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, http://www.dos.ny.gov/consumerprotection, 1-800-697-1220.

For Rhode Island residents: You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes. You may also contact the Rhode Island Office of the Attorney General, 150 South Main Street Providence, Rhode Island 02903, http://www.riag.ri.gov/, (401) 274-4400.

For Tennessee residents:

TENNESSEE CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE

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. A security freeze must be requested in writing by certified mail or by electronic means as provided by a consumer reporting agency. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. If you are actively seeking a new credit, loan, utility, or telephone account,

you should understand that the procedures involved in lifting a security freeze may slow your applications for credit. You should plan ahead and lift a freeze in advance of actually applying for new credit. When you place a security freeze on your credit report, you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or authorize the release of your credit report for a period of time after the freeze is in place. To provide that authorization you must contact the consumer reporting agency and provide all of the following:

1. The personal identification number or password;
2. Proper identification to verify your identity; and
3. The proper information regarding the period of time for which the report shall be available.

A consumer reporting agency must authorize the release of your credit report no later than fifteen (15) minutes after receiving the above information. A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account, that requests information in your credit report for the purposes of fraud control, or reviewing or collecting the account. Reviewing the account includes activities related to account maintenance.

You should consider filing a complaint regarding your identity theft situation with the Federal Trade Commission.