



[January 18], 2023

<First Name> <Last Name>
<Street Address>
<City>, <State> <Zip Code>

NOTICE OF SECURITY INCIDENT

Dear <First Name>,

Protecting the security of our customers’ information is very important to us. We are writing to inform you about an incident that may have impacted your PayPal account. We want to make clear at the outset that keeping your personal data safe and secure is and will continue to be a priority moving forward.

WHAT HAPPENED?

On December 20, 2022, we confirmed that unauthorized parties were able to access your PayPal customer account using your login credentials. We have no information suggesting that any of your personal information was misused as a result of this incident, or that there are any unauthorized transactions on your account. There is also no evidence that your login credentials were obtained from any PayPal systems.

Based on PayPal’s investigation to date, we believe that this unauthorized activity occurred between December 6, 2022, and December 8, 2022, when we eliminated access for unauthorized third parties. During this time, the unauthorized third parties were able to view, and potentially acquire, some personal information for certain PayPal users.

We have not delayed this notification as a result of any law enforcement investigation.

WHAT INFORMATION WAS INVOLVED?

The personal information that was exposed could have included your name, address, Social Security number, individual tax identification number, and/or date of birth.

WHAT WE ARE DOING

Upon learning about this unauthorized activity, we promptly began an investigation and took action to address this incident, including by taking steps to prevent unauthorized actors from obtaining further personal information. We reset the passwords of the affected PayPal accounts and implemented enhanced security controls that will require you to establish a new password the next time you login to your account.

We have also secured the services of Equifax to provide identity monitoring services at no cost to you for two years. Below please find information on signing up for a complimentary membership to Equifax’s identity monitoring services, including key product features.

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ 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 alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- 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 theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

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.

[January 18], 2023
Activation Code: _____
Expiration Date: _____

WHAT YOU CAN DO

We encourage you to contact Equifax and take advantage of the identity monitoring services we are providing to you free of charge. In addition, you should remain vigilant and carefully review your accounts for any suspicious activity.

To further protect yourself, we recommend you take a few steps. For example:

- We recommend you update your passwords for any accounts where you are currently using the same username and password combination as those used for your PayPal account.
- If you detect any suspicious activity on an account, change the password and security questions immediately, and promptly notify the company where the account is maintained.
- You may also add additional security for your PayPal account by enabling “2-step verification” in your Account Settings.
- When links are present in an email, individuals should hover your mouse over the links to view the actual destination URL and should not click on the link if you are unsure of the destination URL or website.
- You should also pay attention to messages that promote an urgency and require immediate action.
- If you are unsure or want to confirm the authenticity of urgent messages, you should visit PayPal.com separately and access their PayPal account to view any messages.
- PayPal will never ask you to provide the username and password of your PayPal account or any authentication factors, such as a one-time code, over a call, text, or an email message.

If you would like to take additional steps to protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations from 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.

FOR MORE INFORMATION

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

If you have any questions, please contact us by clicking: [Help & Contact](#).

Sincerely,

PayPal

¹The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness. ²Credit monitoring from Experian and TransUnion will take several days to begin. ³WebScan 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. ⁴The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ⁵Locking 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.co ⁶The 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.

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, we recommend 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 other 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, and 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 <https://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.

[January 18], 2023
Activation Code:
Expiration Date:

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

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; and 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

[January 18], 2023
Activation Code: _____
Expiration Date: _____

Protection at: 99 Washington Avenue, Albany, New York 12231-0001, <http://www.dos.ny.gov/consumerprotection>, 1-800-697-1220.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington, D.C. 20001, <https://www.oag.dc.gov/>, 202-727-3400.