

[UPGRADE LETTERHEAD WITH ADDRESS]

[CUSTOMER NAME AND ADDRESS]

[DATE]

Notice of Suspicious Activity

Dear [CUSTOMER NAME]:

We are writing to provide you with information regarding suspicious activity on your account with Upgrade, Inc.

What Happened

Around [LOGIN DATE], we detected a suspicious login to your Upgrade account that happened on or around the same date. The suspicious login was performed using your valid login credentials. Based on our review, our systems have not been hacked and your credentials were not stolen from us. However, anyone logged into your account using stolen credentials may be able to view your account information.

What Information Was Involved

Account information, which may include your login credentials, name, date of birth, address, phone number, credit score, and applicant or borrower documentation.

What We Are Doing

Upgrade has disabled your existing password to prevent further suspicious activity and will implement additional security measures. To re-establish your account, please reset your password at www.upgrade.com/portal/forgot-password.

What You Can Do

We recommend that you promptly change your password on all accounts where you may be using the same credentials. You should not use identical usernames and passwords across multiple accounts. We encourage you to take proactive measures now to help prevent and detect any misuse of your information. Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for details.

For More Information

For further information or assistance, you can contact Upgrade by emailing us at resolution@upgrade.com. To speak with an Upgrade Support representative, you may call our toll-free line at (833) 211-5227 Monday-Friday 8am-5pm MST.

Sincerely,
Upgrade, Inc.

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 over the next 12 to 24 months by reviewing your account statements and monitoring 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 any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (1-877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Contact information for the FTC is: 1-877-382-4357, www.ftc.gov, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

· **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, 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 access the request form at www.annualcreditreport.com/manualRequestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for purpose of general enquiries or requesting a copy of your credit report is provided below:

Equifax 1-866-349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian 1-888-397-3742 www.experian.com P.O. Box 2002 Allen, TX 75013	TransUnion 1-833-395-6938 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19016
---	--	---

· **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

· **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the FTC's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (1-877-438-4338).

A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf. A summary of your rights under the Fair Credit Reporting Act can also be found on the FTC's website at www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

If you are a District of Columbia resident: you may also contact the Office of the District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

If you are a Maryland resident: you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at www.marylandattorneygeneral.gov/Pages/IdentityTheft or by sending an email to idtheft@oag.state.md.us or calling 1-410-576-6491. Contact information for the Maryland Attorney General's Office is: 1-888-743-0023, www.marylandattorneygeneral.gov, 200 St. Paul Place, Baltimore, MD 21202.

If you are a North Carolina resident: you may also obtain information about preventing identity theft from the North Carolina Attorney General's Office at www.ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft or at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226 (Toll-free within North Carolina) or 1-919-716-6000.

If you are a New York resident: you may also contact the following state agencies: (i) the NYS Attorney General, 1-800-771-7755, www.ag.ny.gov, (ii) the NYS Office of Information Technology Services, 1-844-891-1786, www.its.ny.gov, and (iii) the Department of State's Division of Consumer Protection, 1-800-697-1220, www.dos.ny.gov.

If you are a Puerto Rico resident: you may also contact the Office of the Attorney General, PO Box 9020192, San Juan, PR, 00902-0192, 1-787-721-2900, www.justicia.pr.gov.

If you are a Rhode Island resident: you may also contact the Office of the Attorney General, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

OTHER IMPORTANT INFORMATION

Security Freeze

A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. A consumer reporting agency may charge you for requesting or removing a security freeze. To place a security freeze, please contact the three credit reporting agencies identified above.