Marcus
by Goldman Sachs®

20274

Goldman Sachs Bank USA
PO Box 1978
Cranberry Twp., PA 16066

000001-01-04

April 28, 2021

[redacted]

Hi [redacted],

At Marcus, we take the security of your account very seriously. We're writing to let you know that we have identified login(s) to your Marcus account that we believe may not have been by you. If the login(s) were not you, this means that certain information of yours would have been accessible to someone else who accessed your account. Below, we explain what we have done and are doing to address this occurrence, and share some steps you can take to help protect yourself. We sincerely regret that this occurred.

For any questions, please call us at **1-855-730-7283**, Monday to Friday, 8 am - 10 pm, or Saturday to Sunday, 9 am - 7 pm ET.

Here's what happened:

As part of our regular monitoring for suspicious activity, we identified one or more successful logins into your account that were not consistent with your past login history. Marcus has security measures in place that enable us to determine typical login behavior for each customer. The activity we identified was not consistent with your typical behavior, which is why we believe it may not have been you. However, we want you to know that based on information currently available to us, there was no breach of Marcus's databases.

Once we became aware of the suspicious login(s), we reviewed your account for suspicious activity or unauthorized transactions. Based on our review, we have not identified any unusual activity or transactions within your account.

Here's how the incident affected your information:

If the login activity was not authorized by you, some of your information would have been accessible to an unauthorized person. The information that would have been accessible includes your name, date of birth, the last four digits of your social security number, your Marcus Savings account number, and the transaction data from external accounts linked via Marcus Insights.

Here's what we are doing to help protect you:

When we first noticed this activity, we locked your account and required a password reset. If you have not reset your password yet, please do so now at marcus.com. We have also put your account under enhanced monitoring for suspicious transactions.

000001/1189589/LTRS/0001/0000/000000/000001 000 01 000000

Here are some things you can do to protect yourself:

- **Anti-Virus Software:** You should ensure your computers and mobile devices have anti-virus software installed that is regularly updated and which periodically scans your device

- **Change Other Account Passwords and Enable Multi-factor Authentication.** If you use the same or similar passwords for other online accounts that you do for Marcus, change your password for those accounts. You should use unique, "strong" passwords for all online accounts. For your personal non-Marcus accounts that support it, enable multi-factor authentication, which requires more than a username and password to access your account. (Multi-factor authentication may include a code texted to your phone, your fingerprint, or a number generated by a token or app.)

- **Suspicious Links:** Do not click on links in emails or texts from senders you don't recognize. You shouldn't assume an unexpected email or text message is authentic. Clicking on a link from a sender you don't know can give fraudsters access to your information. Similarly, exercise caution when clicking links from senders whose name you recognize, because fraudsters may attempt to impersonate known senders. If you doubt the authenticity of an email from Marcus, you may access your Marcus account by navigating directly in your web browser to https://www.marcus.com or via the Marcus application.

- **Don't download software you don't recognize:** Never download software from a source you don't trust. These links often contain software that could give criminals access to your device. If someone has called you unexpectedly claiming to be from your bank or another trusted organization, be wary and never give them access to your device.

- **Financial Accounts.** Review your Marcus and other financial account statements to check for any discrepancies or unusual activity. If you see any account activity that you don't understand, contact the financial institution immediately.

- **Check Credit Reports.** Under U.S. law, you are entitled to one free credit report annually from each of the three nationwide consumer reporting agencies - Experian, Equifax and TransUnion. To order your free reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228. Carefully check your credit reports for any accounts you did not open and for any credit check inquiries that you did not initiate. If you see anything you do not understand, call the agency immediately. If you find fraudulent activity on your credit reports, follow the instructions provided by the agency to report fraud.

- **For more information**, see the enclosed Reference Guide, which sets out information on protecting your personal information and identity, including recommendations from the U.S. Federal Trade Commission.

We take our obligation to safeguard personal information very seriously. We sincerely regret this happened and any inconvenience it may cause you. We value you and appreciate the trust you've placed in us. If you have any questions, please call 1-855-730-7283.

Sincerely,

Marcus by Goldman Sachs

Reference Guide

We encourage our affected customers to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC, and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.
- Report identity theft at www.IdentityTheft.gov

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-FTC-HELP (382-4357)

www.ftc.gov/idtheft/
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. The initial fraud alert remains in place for a year. You can then continue to maintain a fraud alert on your credit file indefinitely by placing a new fraud alert each year. If you experience identity theft, you may request for your initial fraud alert to remain on your credit file for 7 years. You can place a fraud alert on your credit file by calling any one of the toll-free numbers provided below. You only need to call one of the credit reporting agencies – Equifax, Experian or TransUnion. The agency that you notify will alert the other two agencies to also place a fraud alert on your credit file. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-685-1111	www.Equifax.com/personal/credit-report-services
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/help
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-888-909-8872	www.transunion.com/credit-help

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to protect you from identity theft by requiring your express authorization before potential creditors may access your credit file at the consumer reporting agencies. Because a security freeze adds verification steps to the credit reporting process, the freeze may delay, interfere with, or prevent the approval of a loan or other credit you seek to obtain. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above.