2024-249

Marcus by Goldman Sachs

Goldman Sachs Bank USA
PO Box 70379
Philadelphia, PA 19176-0379

[redacted]

[redacted]

Important information about your account

Customer since: [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 have reason to believe were not performed by you. We identified these login(s) as part of our regular monitoring for suspicious activity. Your login credentials were not obtained as a result of a compromise of our systems.

If the login(s) were not performed by you, this means that certain personal information about you would have been accessible to the person who accessed your account, such as your name, Marcus deposit account number, and the details for the virtual card associated with your My GM Rewards Card (i.e., card number, security code and expiration date). Please note that:

- Your Social Security number is not accessible via your online Marcus account and, therefore, was not affected by this issue.
- The virtual card associated with your My GM Rewards Card has a different account number from the physical card.

When we identified the suspicious login(s), we suspended both online access to your account and transfers to or from your deposit account. In addition, we changed the account number for the virtual card, which prevents future transactions using the affected card's details. If you have authorized transactions on your virtual card number, please be mindful that these charges may be declined and you'll need to provide updated card details to the merchant.

We have attempted to contact you by phone. If we have not already spoken with you, we encourage you to call us at 1-855-730-7283 and we'll assist you in further protecting your account.

Sincerely,

Marcus by Goldman Sachs

Chat with us: Log in at marcus.com or call 1-855-730-7283 | 24 hours a day / 7 days a week

000001/1398823/LTRS/0001/0000/000000/000001 000 01 000000

Although we do not know how an unauthorized person may have gained access to your account, there are a variety of steps you may be able to take to help protect yourself:

000001-02-05

- **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. (Multifactor authentication may include a code texted to your phone, your fingerprint, or a number generated by a token or app.)

- **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.

- **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, particularly over the next twelve to twenty-four months, to check for any discrepancies or unusual activity. Promptly report incidents of suspected identity theft or unauthorized transactions to us or the other 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 value you and appreciate the trust you've placed in us. If you have any questions, please call 1-855-730-7283.

Sincerely,

The Marcus Team

Reference Guide

We encourage you to consider taking the following steps:

000001-03-05

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. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol

Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov/

000001-05-05

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/resources/individuals/consumer-issues/technology

Marcus by Goldman Sachs®

Goldman Sachs Bank USA
PO Box 70379
Philadelphia, PA 19176-0379

[redacted]

[redacted]

000001-01-05

Important information about your account

Customer since: [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 have reason to believe were not performed by you. We identified these login(s) as part of our regular monitoring for suspicious activity. Your login credentials were not obtained as a result of a compromise of our systems.

If the login(s) were not performed by you, this means that certain personal information about you would have been accessible to the person who accessed your account, such as your name, Marcus deposit account number. Please note that your Social Security number is not accessible via your online Marcus account and, therefore, was not affected by this issue.

When we identified the suspicious login(s), we suspended both online access to your account and transfers to or from your deposit account.

We have attempted to contact you by phone. If we have not already spoken with you, we encourage you to call us at 1-855-730-7283 and we'll assist you in further protecting your account.

Sincerely,

Marcus by Goldman Sachs

000001/1398822/LTRS/0001/0000/000000/000001 000 01 000000

Although we do not know how an unauthorized person may have gained access to your account, there are a variety of steps you may be able to take to help protect yourself:

000001-02-05

- **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. (Multifactor authentication may include a code texted to your phone, your fingerprint, or a number generated by a token or app.)

- **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.

- **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, particularly over the next twelve to twenty-four months, to check for any discrepancies or unusual activity. Promptly report incidents of suspected identity theft or unauthorized transactions to us or the other 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 value you and appreciate the trust you've placed in us. If you have any questions, please call 1-855-730-7283.

Sincerely,

The Marcus Team

Reference Guide

We encourage you to consider taking the following steps:

000001-03-05

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. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol

Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov/

000001-05-05

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/resources/individuals/consumer-issues/technology

Marcus:
by Goldman Sachs®

gm rewards cards

Goldman Sachs Bank USA
PO Box 70321
Philadelphia PA 19176-0321

[redacted]

January 29, 2024

Important message regarding your account

Dear Ni[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 have reason to believe were not performed by you. We have identified these login(s) as part of our regular monitoring for suspicious activity. Your login credentials were not obtained as a result of a compromise of our systems.

If the login(s) were not performed by you, this means that certain personal information about you would have been accessible to the person who accessed your account, such as your name and the details for the virtual card associated with your GM Card (i.e., card number, security code, and expiration date). Please note that:

- Your Social Security number is not accessible via your online Marcus account and, therefore, was not affected by this issue.
- The virtual card associated with your GM Card has a different account number from the physical card.

We have changed the account number for the virtual card, which prevents future transactions using the affected card's details. If you have authorized transactions on your virtual card number, please be mindful that these charges may be declined and you will need to provide updated card details to the merchant.

Although we do not know how an unauthorized person may have gained access to your account, there are a variety of steps you may be able to take to help protect yourself:

- **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. (Multifactor authentication may include a code texted to your phone, your fingerprint, or a number generated by a token or app.)

- **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.
- **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, particularly over the next twelve to twenty-four months, to check for any discrepancies or unusual activity. Promptly report incidents of suspected identity theft or unauthorized transactions to us or the other 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 value you and appreciate the trust you’ve placed in us. If you have any questions, please call 1-833-773-0988.

We're here to help: 1-833-773-0988 24 hours a day / 7 days a week

Marcus by Goldman Sachs® is a brand of Goldman Sachs Bank USA and Goldman Sachs & Co. LLC, which are subsidiaries of The Goldman Sachs Group, Inc. Goldman Sachs Bank USA, Salt Lake City Branch, is the issuer of the GM Reward Cards. General Motors is solely responsible for the operation and administration of the Earnings Program and Points Program. For more details about the General Motors Earnings Program and Points Program, including redemption options, go to mygmrewardscard.com.

Reference Guide

We encourage you to consider taking 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. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol

Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov/

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/resources/individuals/consumer-issues/technology