LOGO

May 11, 2022

Name
Address
City, State, ZIP

NOTICE OF DATA BREACH

Dear [Name],

We're happy to have you as a Member of the General Motors family, appreciate your loyalty and take the protection of your personal information seriously.

We are writing to follow up on our [DATE] email to you, advising you of a data incident involving the identification of recent redemption of your reward points that appears to be without your authorization. We are investigating and will restore any points that were redeemed without your authorization.

In that email, we also informed you that for you to continue accessing your account, you need to reset your password. If you have not already done so, click on this link and follow the instructions: **Recover GM Account**. This action is necessary to help keep your personal information safe and your account secure.

We want you to understand what happened and the steps we have taken to address the incident. Although we have no reason to believe that any further misuse of the information included in your GM account will occur, we have included suggestions on measures you can take to better protect your account and your personal information.

What Happened
Between April 11, 2022 and April 29, 2022, we identified some suspicious log ins to certain GM online customer accounts and identified recent redemption of customer reward points for gift cards that may have been performed without the customers' authorizations. Upon discovery, we suspended this feature on the account website and notified affected customers of these issues, advising them that they would need to reset their passwords in order to gain access to their online customer accounts. We also reported the activity to law enforcement. We continue to monitor account activity to protect our customers and personal information about them.

What Information Was Involved
Based on the investigation to date, there is no evidence that the log in information was obtained from GM itself. We believe that unauthorized parties gained access to customer login credentials that were previously compromised on other non-GM sites and then reused those credentials on the customer's GM account. Through this unauthorized activity, the unauthorized parties could have gained access to limited personal information of your GM online or mobile application accounts, such as first and last name, personal email address, personal address, username and phone number for registered family members tied to your account, last known and saved favorite location information, your currently subscribed OnStar package (if applicable), family members' avatars and photos (if uploaded), profile picture, search and destination information, reward card activity, and fraudulently redeemed reward points. The GM accounts did **not** include date of birth, Social Security number, driver's license number, credit card

information, or bank account information, as that information is not stored in your GM account.

What We Are Doing
As discussed above, we took swift action in response to the suspicious activity by suspending gift card redemption and notifying affected customers of these issues. We also took steps to require those customers to reset their passwords at their next log in, and we reported this incident to law enforcement.

What You Can Do
If you haven't yet, please follow the steps outlined above to reset your GM password. We recommend, as good security practices, that you not use the same password for different accounts, and that you update any use of duplicate passwords.

Please review the additional resources included with this letter (Attachment A). This attachment describes additional best practices you can take to help protect personal information about you generally, 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.

Placing a Fraud Alert
If you have concerns about possible identity theft, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. You may obtain additional information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report.

Obtain a Police Report
For security incidents generally, you have the right to file and obtain a copy of a police report.

We regret any inconvenience or concern this incident may have caused. If you have any questions concerning this incident, please call the GM toll-free number at (844) 764-2665, Monday through Saturday, 9:00 a.m.-8:00 p.m. Eastern Time.

Sincerely,

[INSERT SIGNATURE]

My GM Account
Connection Center Support

ATTACHMENT A

Order Your Free Credit Report

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus (Equifax, Experian, and TransUnion). To order your free annual 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.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number, or request form. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax www.equifax.com	(800) 685-1111
Experian www.experian.com	(888) 397-3742
TransUnion www.transunion.com	(800) 916-8800

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus 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 credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

We encourage you remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

As a reminder, if you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidence of identity theft or fraud, promptly report the matter to your local law enforcement authorities (from whom you can obtain a police report), state Attorney General, and the Federal Trade Commission (FTC). You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission Bureau of Consumer Protection
600 Pennsylvania Avenue NW Washington, DC 20580
(877) IDTHEFT (438-4338)
www.ftc.gov/idtheft

Placing a Security Freeze
Under the federal Fair Credit Reporting Act, 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, and Social Security number to request a security freeze and may be provided 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. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

https://www.equifax.com/personal/credit-report-services/
https://www.experian.com/freeze/center.html
https://www.transunion.com/credit-freeze

As of April 18, 2022, the reporting agencies allow you to place a credit freeze through the online, physical mail and phone numbers and request that you provide the information listed below. Where possible, please consult the websites listed above for the most up-to-date instructions.

Reporting Agency	**Online**	**Physical Mail**	**Phone Number**
Equifax	***Freeze request may be submitted via your myEquifax account, which you can create here***: https://my.equifax.com/consumer-registration/UCSC/#/personal-info	***Mail the Equifax Freeze Request Form to***: Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 ***Form may be found here***: https://assets.equifax.com/assets/personal/Security_Freeze_Request_Form.pdf	888-298-0045
Experian	***Freeze request may be submitted here***:	***Mail the request to***: Experian Security Freeze, P.O. Box 9554, Allen, TX 75013 ***Request must include:***	888-397-3742

	https://www.experian.com/ncaconline/freeze	• Full Name • Social security number • Complete address for last 2 years • Date of birth • One copy of a government issued identification card, such as a driver's license, state ID card, etc. • One copy of a utility bill, bank or insurance statement, etc.	
TransUnion	***Freeze request may be submitted via your TransUnion account, which you can create here***: https://service.transunion.com/dss/orderStep1_form.page?	***Mail the request to***: TransUnion P.O. Box 160 Woodlyn, PA 19094 ***Request must include:*** • Full Name • Social security number • Complete address	888-909-8872

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.