HUNTON& WILLIAMS

HUNTON & WILLIAMS LLP
2200 PENNSYLVANIA AVENUE, NW
WASHINGTON, D.C. 20037-1701

TEL 202 • 955 • 1500
FAX 202 • 778 • 2201

PAUL M. TIAO
DIRECT DIAL: 202 • 955 • 1618
EMAIL: ptiao@hunton.com

February 9, 2018

Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

In accordance with N.H. Rev. Stat. Ann. § 359-C:20, I am writing to you on behalf of OneMain Financial ("OneMain") to notify you regarding the nature and circumstances of a recent data security incident.

OneMain recently determined that an unauthorized individual(s) apparently compromised the personal or work e-mail accounts of OneMain customers, and used the e-mail accounts between September 1, 2017 and January 16, 2018 to access certain customer's OneMain online accounts. Based on OneMain's review of the incident, it does not appear that OneMain was the source of or responsible for the apparent compromise of customers' personal or work email accounts.

The personal information involved in this incident may have included first and last name, phone number, OneMain loan account number, OneMain Rewards account, and type of insurance purchased for a OneMain loan account, if applicable. For the majority of affected online accounts, OneMain has no evidence to suggest that unauthorized activity took place other than access to this personal information. For some accounts, however, OneMain believes that the unauthorized individual(s) may also have accessed customers' OneMain Rewards accounts or enrolled customers into a OneMain Rewards account, and taken steps to inflate Rewards points and redeem those points for gift cards. In a very limited number of circumstances it appears that, in order to inflate Rewards points, the individual(s) may have made or attempted to make unauthorized payments on OneMain loan accounts from bank accounts associated with customers' OneMain online accounts.

Promptly after learning of the incident, OneMain launched an investigation into the nature and scope of the incident. OneMain retained a leading team of data security experts to conduct a forensic investigation and is assisting law enforcement authorities with their investigation into the individual(s) responsible for this incident. OneMain also took appropriate action to secure its system, block any further unauthorized access, and mitigate the effects of this incident. OneMain is restoring any customer's Rewards points that were subject to an unauthorized redemption, and is refunding any unauthorized payments on OneMain loan accounts.

HUNTON&
WILLIAMS

OneMain first became aware of this incident on or about January 8, 2018. There is 1 New Hampshire resident affected by this incident. Attached for your reference is a copy of the notice being sent to the affected individual via U.S. mail on February 6th. Please do not hesitate to contact me if you have any questions.

Very truly yours,

Paul M Tiao

Paul Tiao, Esq.

Enclosures

P.O. Box 1170
Evansville, IN 47706-1170

February 6, 2018

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

Dear [Insert customer name]:

We are writing to let you know that your personal or work email account (for example, john.doe@gmail.com) associated with your OneMain online account may have been compromised and may have been later used by an unauthorized individual(s) between September 1, 2017 and January 16, 2018 to access your OneMain online account.

Promptly after learning of this potential unauthorized access to OneMain online accounts, we took steps to review our systems and determine the nature of this incident. We retained a leading team of independent data security experts to conduct a forensic investigation of this incident and are assisting law enforcement authorities with their investigation into the individual(s) responsible.

Based on our review, it does not appear that OneMain was the source of or responsible for the apparent compromise of your personal or work email account. However, we take our obligation to safeguard your personal information very seriously and are letting you know about this incident so you can take steps to protect yourself.

Your OneMain online account contains certain personal information, including for example the following:

- Your name, address, and phone number;
- Your OneMain loan account number and, if you are enrolled, your OneMain Rewards account; and
- If you purchased insurance, the type of insurance purchased.[1]

To prevent further unauthorized access, we have locked your OneMain online account by requiring you to reset your security questions. If you have not already done so, you should call OneMain Customer Service (1-800-325-2146) for assistance in updating this information the next time you access your OneMain online account.

We recommend that you carefully review your OneMain online account and notify the OneMain Executive Office of Customer Care (1-800-525-6053) of any unauthorized changes or suspicious activity. We also recommend that you change the password for the email account associated with your OneMain online account since it appears to have been used by the unauthorized individual(s) in this incident.

---

[1] Such insurance may be through the following providers: American Health and Life Insurance Company; Triton Insurance Company; Merit Life Insurance Co.; Yosemite Insurance Company; or in New York only, Securian Life Insurance Company.

OneMain Loan Account

Based on our review, we believe that unauthorized payments may have been made on your OneMain loan account from a bank account associated with your OneMain online account. We recommend that you review your recent OneMain loan account statements and contact us immediately about any unauthorized payments. We will work with you to refund any unauthorized payments.

If you have any questions regarding this incident, please call us toll-free at **1-800-525-6053**, Monday through Friday from 8:00 A.M. to 5:00 P.M. Central Time. In addition, the attached Reference Guide provides recommendations by the U.S. Federal Trade Commission on the protection of personal information. We hope this information is useful to you.

We regret any inconvenience this may cause you.

Sincerely,

OneMain Financial
Executive Office of Customer Care

Reference Guide

We encourage our affected customers to take the following steps:

Order Your Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, 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. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.

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.

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

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. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. 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	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	www.transunion.com

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 prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. *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. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

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 military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

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 charge you a fee of up to $5 to place a security freeze on your account, and 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. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
http://www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400
http://www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $10 to place a security freeze on your account, and 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 for a security freeze. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.