NELSON MULLINS

NELSON MULLINS RILEY & SCARBOROUGH LLP
ATTORNEYS AND COUNSELORS AT LAW

106 S. President St., Suite 400
Jackson, MS 39201
M: 404.322.6000 F: 404.322.6050
nelsonmullins.com

Brad C. Moody
T: (601) 278-2118
brad.moody@nelsonmullins.com

September 27, 2021

Attorney General Gordon J. MacDonald
Office of New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, New Hampshire 03301
DOJ-CPB@doj.nh.gov

Re: *MoneyLion Inc. - Notice of Data Incident*

Dear Attorney General MacDonald,

I serve as outside legal counsel to MoneyLion Inc. ("MoneyLion"), which is a technology company with principal offices located at 30 West 21st St, 9th Floor, New York, NY 10010.[1] This correspondence is to notify you of a recent incident involving certain MoneyLion accounts.[2] Specifically, MoneyLion detected an unusual increase in the amount of activity on the MoneyLion platform beginning on or about June 29, 2021. Similar activity was also observed from July 13-16, 2021, and again from July 27-30, 2021.

MoneyLion promptly investigated and determined that an unauthorized outside party appears to have been attempting to gain access to user accounts on the application using login credentials that were potentially compromised in a prior event on another site unrelated to MoneyLion. In some instances, the threat actor(s) was able to use these compromised credentials to successfully gain access to users' accounts and complete transactions without authorization. Importantly, however, MoneyLion believes it has identified affected accounts and made affected users whole if there were any unauthorized transactions. There is also no evidence that users' credentials were obtained from MoneyLion's information technology systems. While MoneyLion cannot definitively identify the source of the compromised emails/passwords at this time, compromised credentials are frequently traded on the dark web among potential threat actors who may attempt to use them to gain access to other accounts.

In response to this incident, MoneyLion proactively secured (locked) the impacted accounts and, beginning on July 18, 2021, sent email notices to affected accountholders. MoneyLion has also worked to preemptively identify and reverse any unauthorized transactions

[1] By providing this notice, MoneyLion does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

[2] MoneyLion has not notified law enforcement of this incident.

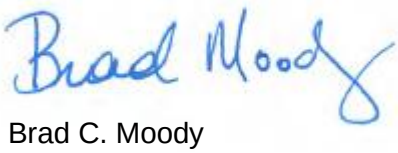
and has been engaging with impacted users directly to address any concerns. Outside experts were engaged to assist MoneyLion with the investigation and the identification of any potentially affected accounts. MoneyLion also has implemented additional multi-factor authentication for all accounts.

Though the source of the compromise did not originate at MoneyLion, in an abundance of caution, notification letters are being sent via U.S. Mail to 3 residents of your State on or about September 24, 2021. Sample notification letters are enclosed for your reference and include the following:

- A description of the event;
- Steps taken to investigate;
- Steps taken to mitigate any potential harm to consumers;
- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this event, etc.

MoneyLion and its banking partner MetaBank are fully committed to protecting consumer privacy and the confidentiality of personal information. We will follow-up this correspondence with any forms or other documents that may need to be completed. Please contact me if you require any additional information regarding this incident.

Best regards,



Brad C. Moody

Enclosure:
Exhibits:
Sample Notification Letter 1 sent to 1 residents
Sample Notification Letter 2 sent to 0 residents
Sample Notification Letter 3 sent to 2 residents

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

This supplemental notification is being sent to you in connection with the suspicious activity that was recently detected on your MoneyLion account and to provide information regarding additional steps you may want to consider to restore and protect your account. Between July 18 – 29, we emailed notices to you and other potentially impacted customers about unusual activity that had been detected on the MoneyLion application. We, along with our banking partner, are now providing this further notice to you.

What happened? Beginning on or about June 29, we detected unusual activity on the MoneyLion platform. MoneyLion promptly started an investigation and determined that a very limited number of accounts were potentially impacted. Similar activity occurred again between July 13 – 16, and once again between July 27 – 30. Through our investigation, we have determined that an unauthorized outside party appears to have been attempting to gain access to your account on the application using an account password and/or possibly email address that appear to have been potentially compromised in a prior event on another site unrelated to MoneyLion. **Importantly, there is no evidence that your credentials were obtained from MoneyLion's information technology systems.** While we cannot definitively identify the source of the compromised email/password at this time, compromised credentials are frequently traded on the dark web among potential threat actors who may attempt to use them to gain access to other accounts.

What information was involved? It is important to note that there is **no evidence** that your Social Security Number, driver's license number, details for any linked bank accounts or linked debit card number(s) were affected, but it does appear that an unauthorized outside party used your password to access your account and may have withdrawn funds, taken out loans, received cash advances, transferred funds and/or made payments using your external accounts. As previously advised, MoneyLion has mitigated or is still attempting to resolve any unauthorized transactions that may have been processed on your account. **You will not incur any financial loss from this event.**

What we are doing? There is no evidence to date of any intrusion into MoneyLion's systems beyond access to your individual account and certain other users' accounts via previously compromised credentials. In response to this event, we have secured (locked) the impacted accounts and sent email notices to affected customers. If you reset your password after receiving the prompting email, your MoneyLion services should have been restored. Outside experts are engaged to assist MoneyLion with the investigation, ongoing remediation efforts and the identification of any potentially affected accounts. Additionally, as you may be aware, we also have implemented additional multi-factor authentication for all accounts.

What can you do? While MoneyLion has secured your account, if you have not already done so, you will need to reset your password that meets MoneyLion's security requirements to gain access to your account. You can create this new password by using the Forgot Password link on your login screen. We strongly recommend you use a unique password that you have not used on other sites. As always, we recommend that you remain vigilant to fraud and that you always use unique passwords for all websites and applications – and update those passwords often, storing them in a secure location. We also have enclosed some additional steps that you can consider taking, as you deem appropriate.

For more information, please call MoneyLion's support service number for this event at 1-855-651-2706 between the hours of Monday – Friday 9:00 a.m. to 6:30 p.m. Eastern Time excluding major U.S. holidays. MoneyLion is fully committed to protecting your personal information and is continuing to take steps to enhance security measures to help reduce the risk of something like this happening in the future.

Sincerely –

Jess Jackson

Director of Customer Operations

Additional Steps You May Wish to Take:

- **FREEZE YOUR CREDIT FILE.** 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. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:
    - *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
    - *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
    - *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

- **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, 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 1-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 an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

- **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain 1 free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the 3 credit reporting agencies directly to obtain such additional reports.)
    - *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
    - *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
    - *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

- **POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it. Notification of this incident has not been delayed as a result of a law enforcement investigation.

- **FAIR CREDIT REPORTING ACT (FCRA):** Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. 1) You must be told if information in your file has been used against you. 2) You have the right to know what is in your file. 3) You have the right to ask for a credit score. 4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. 6) Consumer reporting agencies may not report outdated negative information. 7) Access to your file is limited. 8) You must give your consent for reports to be provided to employers. 9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. 10) 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. 11) You may seek damages from violators. 12) Identity theft victims and active duty military personnel have additional rights.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT, FRAUD ALERTS, SECURITY FREEZES AND FCRA FROM THE FEDERAL TRADE COMMISSION.** Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html. Federal Trade Commission also provides information at www.ftc.gov/idtheft. FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM YOUR STATE ATTORNEY GENERAL.**
  - *Maryland: You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-410-528-8662; www.oag.state.md.us Consumer Hotline1-410-528-8662, or consumer@oag.state.md.us.*
  - *Connecticut: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag*
  - *District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, 1-202-727-3400, databreach@dc.gov, www.oag.dc.gov.*
  - *Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html*
  - *New York: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-6971220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov*
  - *North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000/ 1-877-566-7226, www.ncdoj.gov*
  - *Rhode Island: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov. (Approximately # Rhode Island residents were impacted by this incident.)*

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

This supplemental notification is being sent to you in connection with the suspicious activity that was recently detected on your MoneyLion account and to provide information regarding additional steps you may want to consider to restore and protect your account. Between July 18 – 29, we emailed notices to you and other potentially impacted customers about unusual activity that had been detected on the MoneyLion application. We, along with our banking partner, are now providing this further notice to you.

What happened? Beginning on or about June 29, we detected unusual activity on the MoneyLion platform. MoneyLion promptly started an investigation and determined that a very limited number of accounts were potentially impacted. Similar activity occurred again between July 13 – 16, and once again between July 27 – 30. Through our investigation, we have determined that an unauthorized outside party appears to have been attempting to gain access to your account on the application using an account password and/or possibly email address that appear to have been potentially compromised in a prior event on another site unrelated to MoneyLion. **Importantly, there is no evidence that your credentials were obtained from MoneyLion's information technology systems.** While we cannot definitively identify the source of the compromised email/password at this time, compromised credentials are frequently traded on the dark web among potential threat actors who may attempt to use them to gain access to other accounts.

What information was involved? It is important to note that there is **no evidence** that your Social Security Number, driver's license number, details for any linked bank accounts, or linked debit card number(s) were affected, but it does appear that an unauthorized outside party used your password to access your account. As previously advised, MoneyLion has mitigated the unauthorized access and also has issued you a new RoarMoney virtual debit card number as a precaution. **You will not incur any financial loss from this event.**

What we are doing? There is no evidence to date of any intrusion into MoneyLion's systems beyond access to your individual account and certain other users' accounts via previously compromised credentials. In response to this event, we have secured (locked) the impacted accounts and sent email notices to affected customers. If you reset your password after receiving the prompting email, your MoneyLion services should have been restored. Outside experts are engaged to assist MoneyLion with the investigation, ongoing remediation efforts and the identification of any potentially affected accounts. Additionally, as you may be aware, we also have implemented additional multi-factor authentication for all accounts.

What can you do? While MoneyLion has secured your account, if you have not already done so, you will need to reset your password that meets MoneyLion's security requirements to gain access to your account. You can create this new password by using the Forgot Password link on your login screen. We strongly recommend you use a unique password that you have not used on other sites. As always, we recommend that you remain vigilant to fraud and that you always use unique passwords for all websites and applications – and update those passwords often, storing them in a secure location. We also have enclosed some additional steps that you can consider taking, as you deem appropriate.

For more information, please call MoneyLion's support service number for this event at 1-855-651-2706 between the hours of Monday – Friday 9:00 a.m. to 6:30 p.m. Eastern Time excluding major U.S. holidays. MoneyLion is fully committed to protecting your personal information and is continuing to take steps to enhance security measures to help reduce the risk of something like this happening in the future.

Sincerely –

Jess Jackson

Director of Customer Operations

Additional Steps You May Wish to Take:

- **FREEZE YOUR CREDIT FILE.** 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. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:
    - *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
    - *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
    - *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

- **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, 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 1-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 an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

- **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain 1 free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the 3 credit reporting agencies directly to obtain such additional reports.)
    - *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
    - *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
    - *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

- **POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it. Notification of this incident has not been delayed as a result of a law enforcement investigation.

- **FAIR CREDIT REPORTING ACT (FCRA):** Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. 1) You must be told if information in your file has been used against you. 2) You have the right to know what is in your file. 3) You have the right to ask for a credit score. 4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. 6) Consumer reporting agencies may not report outdated negative information. 7) Access to your file is limited. 8) You must give your consent for reports to be provided to employers. 9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. 10) 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. 11) You may seek damages from violators. 12) Identity theft victims and active duty military personnel have additional rights.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT, FRAUD ALERTS, SECURITY FREEZES AND FCRA FROM THE FEDERAL TRADE COMMISSION.** Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html. Federal Trade Commission also provides information at www.ftc.gov/idtheft. FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM YOUR STATE ATTORNEY GENERAL.**
  - *Maryland: You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-410-528-8662; www.oag.state.md.us Consumer Hotline1-410-528-8662, or consumer@oag.state.md.us.*
  - *Connecticut: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag*
  - *District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, 1-202-727-3400, databreach@dc.gov, www.oag.dc.gov.*
  - *Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html*
  - *New York: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-6971220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov*
  - *North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000/ 1-877-566-7226, www.ncdoj.gov*
  - *Rhode Island: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov. (Approximately # Rhode Island residents were impacted by this incident.)*

MoneyLion

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

This supplemental notification is being sent to you in connection with the suspicious activity that was recently detected on your MoneyLion account and to provide information regarding additional steps you may want to consider to restore and protect your account. Between July 18 – 29, we emailed notices to you and other potentially impacted customers about unusual activity that had been detected on the MoneyLion application. We are now providing this further notice to you.

What happened? Beginning on or about June 29, we detected unusual activity on the MoneyLion platform. MoneyLion promptly started an investigation and determined that a very limited number of accounts were potentially impacted. Similar activity occurred again between July 13 – 16, and once again between July 27 – 30. Through our investigation, we have determined that an unauthorized outside party appears to have been attempting to gain access to your account on the application using an account password and/or possibly email address that appear to have been potentially compromised in a prior event on another site unrelated to MoneyLion. **Importantly, there is no evidence that your credentials were obtained from MoneyLion's information technology systems.** While we cannot definitively identify the source of the compromised email/password at this time, compromised credentials are frequently traded on the dark web among potential threat actors who may attempt to use them to gain access to other accounts.

What information was involved? It is important to note that there is **no evidence** that your Social Security Number, driver's license number, details for any linked bank accounts or linked debit card number(s) were affected, but it does appear that an unauthorized outside party used your password to access your account. At this time, we have no evidence that your account experienced any financial fraud as a result of this incident.

What we are doing? There is no evidence to date of any intrusion into MoneyLion's systems beyond access to your individual account and certain other users' accounts via previously compromised credentials. In response to this event, we have secured (locked) the impacted accounts and sent email notices to affected customers. If you reset your password after receiving the prompting email, your MoneyLion services should have been restored. Outside experts are engaged to assist MoneyLion with the investigation, ongoing remediation efforts and the identification of any potentially affected accounts. Additionally, as you may be aware, we also have implemented additional multi-factor authentication for all accounts.

What can you do? While MoneyLion has secured your account, if you have not already done so, you will need to reset your password that meets MoneyLion's security requirements to gain access to your account. You can create this new password by using the Forgot Password link on your login screen. We strongly recommend you use a unique password that you have not used on other sites. As always, we recommend that you remain vigilant to fraud and that you always use unique passwords for all websites and applications – and update those passwords often, storing them in a secure location. We also have enclosed some additional steps that you can consider taking, as you deem appropriate.

For more information, please call MoneyLion's support service number for this event at 1-855-651-2706 between the hours of Monday – Friday 9:00 a.m. to 6:30 p.m. Eastern Time excluding major U.S. holidays. MoneyLion is fully committed to protecting your personal information and is continuing to take steps to enhance security measures to help reduce the risk of something like this happening in the future.

Sincerely –

Jess Jackson

Director of Customer Operations

Additional Steps You May Wish to Take:

- **FREEZE YOUR CREDIT FILE.** 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. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:
    - *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
    - *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
    - *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

- **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, 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 1-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 an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

- **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain 1 free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the 3 credit reporting agencies directly to obtain such additional reports.)
    - *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
    - *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
    - *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

- **POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it. Notification of this incident has not been delayed as a result of a law enforcement investigation.

- **FAIR CREDIT REPORTING ACT (FCRA):** Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. 1) You must be told if information in your file has been used against you. 2) You have the right to know what is in your file. 3) You have the right to ask for a credit score. 4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. 6) Consumer reporting agencies may not report outdated negative information. 7) Access to your file is limited. 8) You must give your consent for reports to be provided to employers. 9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. 10) 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. 11) You may seek damages from violators. 12) Identity theft victims and active duty military personnel have additional rights.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT, FRAUD ALERTS, SECURITY FREEZES AND FCRA FROM THE FEDERAL TRADE COMMISSION.** Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html. Federal Trade Commission also provides information at www.ftc.gov/idtheft. FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM YOUR STATE ATTORNEY GENERAL.**
  - *Maryland: You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-410-528-8662; www.oag.state.md.us Consumer Hotline1-410-528-8662, or consumer@oag.state.md.us.*
  - *Connecticut: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag*
  - *District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, 1-202-727-3400, databreach@dc.gov, www.oag.dc.gov.*
  - *Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html*
  - *New York: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-6971220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov*
  - *North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000/ 1-877-566-7226, www.ncdoj.gov*
  - *Rhode Island: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov. (Approximately # Rhode Island residents were impacted by this incident.)*