

RECEIVED

AUG 10 2017

August 9, 2017

CONSUMER PROTECTION

Gordon J. MacDonald,
New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: New Hampshire Retirement System

Dear Attorney General MacDonald,

McLane Middleton, P.A. represents New Hampshire Retirement System ("NHRS"). The purpose of this letter is to formally notify you about a data security incident that affected forty-five NHRS retirees, 43 of whom are currently residents of the State of New Hampshire.

On Friday, July 21, 2017, NHRS learned that, earlier in the month, an unidentified, unauthorized party established online accounts in the NHRS "My Account" function, which is an Internet portal for members and retirees that provides online accounts for members and retirees to access their pension data. The party who engaged in this activity did so in an attempt to redirect pension payments to unauthorized accounts established at Green Dot Bank, a special purpose financial institution whose business primarily consists of issuing pre-paid debit cards. Because NHRS identified the attempted fraud before any pension payments were made for July, no payments were diverted and no pension funds were affected.

Upon learning of this incident, NHRS immediately reported it verbally to the paralegal in your office responsible for intake of these types of matters, as well as to Robert Adams in the Financial Crimes Division of your office. NHRS also reported this incident to appropriate Special Agents at the United States Secret Service and to the New Hampshire State Police.

Additionally, NHRS immediately shut down the My Account function to prevent any continued unauthorized access and deactivated the fraudulently created My Accounts. NHRS also terminated any fraudulently created electronic direct deposit instructions and issued July pension payments for the affected retirees via paper checks sent through U.S. Mail.

When the party who engaged in this activity established the fraudulent My Accounts, the party would have had access to certain information in the My Account function including the numbers of the retirees' bank accounts where NHRS was making electronic deposits of pension payments. Importantly, social security numbers (SSNs) are not accessible in the My Account function. My Account also does not provide access to any other financial account numbers, governmental identification numbers, or, except for named beneficiary information, other personal information related to members or retirees that is not otherwise publicly available.

Because the party who engaged in this activity would have had access to the bank account numbers of the affected retirees via My Account, NHRS advised them by telephone and in writing that they should immediately notify their banks of this incident and initiate a fraud alert on their accounts. Templates of the two types of notice sent to affected NHRS' New Hampshire retirees are enclosed for your review.

NHRS also contacted Green Dot Bank and facilitated the closure of the fraudulently created Green Dot Bank accounts.

While this incident does not indicate that the full SSN of any NHRS members or retirees was compromised, the party who engaged in this activity certainly had the last four digits of SSNs, and might have had access to the full SSNs through sources outside of NHRS. As a result, to be cautious, NHRS advised the affected individuals to promptly take steps to protect themselves from identity theft, including instituting a credit freeze or establishing credit monitoring with the three major credit service bureaus, Equifax, Experian and TransUnion. NHRS offered to reimburse the retirees for the cost of any credit freeze and has pre-paid for two years of credit monitoring for all affected retirees, who were notified via a letter dated July 25, 2017, about how to activate the credit monitoring through Equifax.

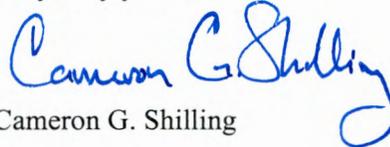
Moreover, NHRS immediately instructed us, as its counsel, to investigate and advise NHRS about this incident and data security more generally. In addition, NHRS retained a computer forensic firm, Charles River Associates, to assist with the investigation and advise NHRS about measures that may be necessary or appropriate to address this situation. Based on their investigation, NHRS' counsel and Charles River Associates concluded that there was no evidence that the information used to create the fraudulent My Accounts originated or was obtained from NHRS or its systems. Rather, it appears that the party who engaged in this conduct obtained the information to create such accounts (name, address, date of birth, and the last four digits of the retiree's SSN) from another source.

After concluding the investigation, and with the assistance of us and Charles River Associates, NHRS posted a notice on its website about this incident and followed that notice with a further email newsletter to its subscriber list of over 40,000 members, retirees and other stakeholders, informing them of the incident and offering guidance on protecting personal information against fraudulent activity.

While NHRS has once again made the My Account function available online for those members and retirees with active accounts, it has not reactivated the part of the portal used to create a new My Account. NHRS will only reinstate the function for establishing a My Account after it implements more stringent security protocols for creating such an account. In addition, NHRS is working with its counsel and forensic company to identify other potentially appropriate remediation and data security measures generally.

We trust that this letter provides you with the information you need to assess this matter, and we are happy to address any questions or concerns you may have.

Very truly yours,



Cameron G. Shilling

Enclosures

cc: New Hampshire Retirement System (w/enclosures)



New Hampshire Retirement System
54 Regional Drive, Concord, NH 03301
Phone: (603) 410-3500 - Fax: (603) 410-3501
Website: www.nhrs.org - Email: info@nhrs.org

July 24, 2017

[REDACTED]
[REDACTED]
[REDACTED] NH 03 [REDACTED]

Re: Data Security Incident

Dear [REDACTED],

The purpose of this letter is to notify you about a data security incident experienced by the New Hampshire Retirement System (NHRS). You are receiving this notice because you are affected by the data security incident.

On Friday, July 21, 2017, NHRS learned that an unidentified, unauthorized party established a number of online accounts in early July in NHRS' "My Account" system, which is our web portal for retirees like you. The My Account system provides individual online accounts for members and retirees to access pension data. The party who engaged in this activity did so in an attempt to redirect pension payments to unauthorized accounts at a financial institution called "Green Dot Bank." Because NHRS identified the attempted fraud before any pension payment was made for July, **no payment was diverted and no pension funds were affected.**

NHRS immediately initiated an investigation. NHRS also has reported this incident to state and federal law enforcement agencies and is fully cooperating with the appropriate authorities. Based on initial information, it appears fewer than 50 NHRS retirees are affected, including you. All affected individuals had not previously established a My Account.

To establish a My Account, the party who engaged in this activity entered the retiree's last name, home zip code, date of birth, and the last four digits of his or her social security number (SSN). Thus, this party had this information about you. NHRS believes that the party did not obtain the information from NHRS, but rather from another unknown source.

Once a My Account was established in your name, the party who created the account could access pension data concerning you and could submit online forms, including an Electronic Direct Deposit (EDD) form. An EDD form is used to initiate direct deposit. That is what occurred to the individuals affected here, including you. Because all EDD forms are manually reviewed and processed by NHRS staff, no changes were finalized. You will receive your July pension check via U.S. Mail as usual.

Upon learning of this incident, NHRS shut down the My Account system to prevent any continued unauthorized access to your information. NHRS has since deactivated your fraudulently created My Account.

When the party who engaged in this activity established a My Account in your name, the party would have had access to certain information in the My Account. Importantly, your full SSN was not accessible on My Account. Nor did the My Account contain any financial account number, governmental identification number, or other personal information related to you that is not otherwise available through public sources.

NHRS suggests that you immediately contact Green Dot Bank to close any account that may have been established in your name with that bank. The customer service contact number for Green Dot Bank is (866) 795-7597. The number of the Green Dot account which was created is: 302794126862.

While NHRS has no evidence that your full SSN was compromised, the party who engaged in this activity certainly had the last four digits of your SSN, and may have your full SSN. To be cautious, NHRS suggests that you promptly take steps to protect yourself from identity theft. Specifically, NHRS suggests that you implement a security freeze on your credit account with each of the three credit reporting agencies identified below. Placing a freeze on your credit accounts will prevent third parties from accessing your credit reports and obtaining credit in your name without your permission. With a security freeze in place, you will receive a personal identification number (PIN) that you will use to obtain information about your credit report and give permission to a third party to access your credit report and initiate credit in your name. If you opt to initiate a security freeze within 60 days, NHRS will reimburse you for the costs of such a security freeze for two years, upon submission of receipts for such costs to the NHRS address provided below.

NHRS cannot initiate a security freeze for you, nor will the credit reporting agencies communicate with NHRS on your behalf. The contact information to initiate a security freeze with the credit reporting agencies is set forth below. If you choose to take this step, you will need to contact each of the three agencies to initiate a security freeze with each agency.

Experian Security Freeze Center
P.O. Box 9554, Allen, TX 75013
(888) 397-3742
www.experian.com/freeze/center.html

Equifax Security Freeze
P.O. Box 105788, Atlanta, GA 30348
(800) 685-1111
www.freeze.equifax.com/Freeze

TransUnion Fraud Victim Assistance Department
P.O. Box 6790, Fullerton, CA 92834
(800) 680-7289
www.transunion.com/credit-freeze/place-credit-freeze

In addition, if you would like to take further precautions to protect your identity beyond initiating a security freeze, NHRS will secure on your behalf and pay for credit monitoring for you for two years. Please contact us if you are interested in having NHRS secure credit monitoring for you.

If you have questions about the incident, or would like assistance with this matter, please contact NHRS at:

Address: 54 Regional Drive, Concord, NH 03301
Phone: Tim Crutchfield 410-3526 or Mark Cavanaugh 410-3592
Email: customercare@nhrs.org

NHRS assures you that we are serious about the privacy and security of our retirees' personal information and pension funds. Accordingly, NHRS will be implementing measures to ensure stricter authentication controls for establishing My Accounts. In addition, NHRS has retained legal counsel and computer security forensic experts to assist NHRS to further investigate this incident and identify measures to enhance our data security protocols.

We sincerely apologize for any inconvenience this incident may cause for you. Please be assured that we are here to help you work through this matter. Thank you.

Yours,

A handwritten signature in black ink, appearing to read "G. P. Lagos", with a horizontal line extending from the end of the signature.

George P. Lagos
Executive Director
New Hampshire Retirement System

Enclosures – EDD Form; return envelope



New Hampshire Retirement System
54 Regional Drive, Concord, NH 03301
Phone: (603) 410-3500 - Fax: (603) 410-3501
Website: www.nhrs.org - Email: info@nhrs.org

July 24, 2017

[REDACTED]
[REDACTED]
[REDACTED] NH 03 [REDACTED]

Re: Data Security Incident

Dear [REDACTED],

The purpose of this letter is to notify you about a data security incident experienced by the New Hampshire Retirement System (NHRS). You are receiving this notice because you are affected by the data security incident.

On Friday, July 21, 2017, NHRS learned that an unidentified, unauthorized party established a number of online accounts in early July in NHRS' "My Account" system, which is our web portal for retirees like you. The My Account system provides individual online accounts for members and retirees to access pension data. The party who engaged in this activity did so in an attempt to redirect pension payments to unauthorized accounts at a financial institution called "Green Dot Bank." Because NHRS identified the attempted fraud before any pension payment was made for July, **no payment was diverted and no pension funds were affected.**

NHRS immediately initiated an investigation. NHRS also has reported this incident to state and federal law enforcement agencies and is fully cooperating with the appropriate authorities. Based on initial information, it appears fewer than 50 NHRS retirees are affected, including you. All affected individuals had not previously established a My Account.

To establish a My Account, the party who engaged in this activity entered the retiree's last name, home zip code, date of birth, and the last four digits of his or her social security number (SSN). Thus, this party had this information about you. NHRS believes that the party did not obtain the information from NHRS, but rather from another unknown source.

Once a My Account was established in your name, the party who created the account could access pension data concerning you and could submit online forms, including an Electronic Direct Deposit (EDD) form. An EDD form is used to request changes to the account and/or financial institution where the retiree's pension payments are deposited. That is what occurred to the individuals affected here, including you. Because all EDD change forms are manually reviewed and processed by NHRS staff, no changes were finalized.

Upon learning of this incident, NHRS shut down the My Account system to prevent any continued unauthorized access to your information. NHRS has since deactivated your fraudulently created My Account.

As a precaution, NHRS has terminated your existing EDD information. NHRS will issue your July pension payment to you via a paper check sent through U.S. Mail. To re-establish your direct deposit, please submit the enclosed EDD form to NHRS in the enclosed return envelope.

When the party who engaged in this activity established a My Account in your name, the party would have had access to certain information in the My Account, including the number of the bank account(s)

where NHRS was making electronic deposits of pension payments for you. Importantly, your full SSN was not accessible on My Account. Nor did the My Account contain any other financial account number, governmental identification number, or other personal information related to you that is not otherwise available through public sources.

Because the party who engaged in this activity would have had access to the account number of the bank account where NHRS was making your electronic deposits, you should immediately notify that bank of this incident and initiate a fraud alert on that account.

In addition to contacting your bank, NHRS suggests that you immediately contact Green Dot Bank to close any account that may have been established in your name with that bank. The customer service contact number for Green Dot Bank is (866) 795-7597. The number of the Green Dot account which was created is: 301749800103.

While NHRS has no evidence that your full SSN was compromised, the party who engaged in this activity certainly had the last four digits of your SSN, and may have your full SSN. To be cautious, NHRS suggests that you promptly take steps to protect yourself from identity theft. Specifically, NHRS suggests that you implement a security freeze on your credit account with each of the three credit reporting agencies identified below. Placing a freeze on your credit accounts will prevent third parties from accessing your credit reports and obtaining credit in your name without your permission. With a security freeze in place, you will receive a personal identification number (PIN) that you will use to obtain information about your credit report and give permission to a third party to access your credit report and initiate credit in your name. If you opt to initiate a security freeze within 60 days, NHRS will reimburse you for the costs of such a security freeze for two years, upon submission of receipts for such costs to the NHRS address provided below.

NHRS cannot initiate a security freeze for you, nor will the credit reporting agencies communicate with NHRS on your behalf. The contact information to initiate a security freeze with the credit reporting agencies is set forth below. If you choose to take this step, you will need to contact each of the three agencies to initiate a security freeze with each agency.

Experian Security Freeze Center
P.O. Box 9554, Allen, TX 75013
(888) 397-3742
www.experian.com/freeze/center.html

Equifax Security Freeze
P.O. Box 105788, Atlanta, GA 30348
(800) 685-1111
www.freeze.equifax.com/Freeze

TransUnion Fraud Victim Assistance Department
P.O. Box 6790, Fullerton, CA 92834
(800) 680-7289
www.transunion.com/credit-freeze/place-credit-freeze

In addition, if you would like to take further precautions to protect your identity beyond initiating a security freeze, NHRS will secure on your behalf and pay for credit monitoring for you for two years. Please contact us if you are interested in having NHRS secure credit monitoring for you.

If you have questions about the incident, or would like assistance with this matter, please contact NHRS at:

Address: 54 Regional Drive, Concord, NH 03301
Phone: Tim Crutchfield 410-3526 or Mark Cavanaugh 410-3592
Email: customercare@nhrs.org

NHRS assures you that we are serious about the privacy and security of our retirees' personal information and pension funds. Accordingly, NHRS will be implementing measures to ensure stricter authentication controls for establishing My Accounts. In addition, NHRS has retained legal counsel and computer security forensic experts to assist NHRS to further investigate this incident and identify measures to enhance our data security protocols.

We sincerely apologize for any inconvenience this incident may cause for you. Please be assured that we are here to help you work through this matter. Thank you.

Yours,

A handwritten signature in black ink, appearing to read "G. P. Lagos", with a horizontal line extending from the end of the signature.

George P. Lagos
Executive Director
New Hampshire Retirement System

Enclosures – EDD Form; return envelope