Celink™
Your Reverse Mortgage Ally

July 3, 2019

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Dear Attorney General MacDonald:

Pursuant to N.H. Rev. Stat. Ann § 359-C:20, we are writing to notify you of a data security incident involving one New Hampshire resident.

Compu-Link Corporation, dba Celink ("Celink") is a Michigan-based servicer and subservicer of reverse mortgage loans. Celink provides this notice in its corporate capacity and as subservicer for Finance of America Reverse LLC for a loan relating to the aforementioned New Hampshire resident.

On June 3, 2019, Celink was the target of a phishing attempt by an outside party in the form of an email to Celink employees that appeared to be from a company in our industry. It contained a link that appeared to be for a secure, encrypted message. When a few Celink employees clicked on the link to open the secure message, the outside party gained temporary access to three employee email boxes. Celink promptly terminated the access and secured these three employee email boxes. A small amount of electronic data could have been accessed by the outside party, including some names, addresses, partial Social Security numbers (the last four digits only), and Celink administrative numbers. The data accessed did not include any security codes, access codes, passwords, complete social security numbers, debit or credit card numbers, or bank account numbers. Celink promptly notified the Michigan State Police of the incident. The Michigan State Police is investigating the incident and took steps to prevent further third-party access to the data. Celink is unaware of any instances of identity theft, fraud, or financial losses associated with the incident.

Celink is preparing notifications about the incident that it plans to send by United States Postal Service First-Class mail to 1 New Hampshire resident. The Michigan State Police has requested that no notification to individuals be made pending the criminal investigation. Once a determination is made by the Michigan State Police that notifying individuals of the incident will not impede the criminal investigation, Celink will provide notice of the incident to the affected individuals. A copy of the information Celink plans to send to the affected New Hampshire resident is attached to this letter.

Celink has taken several steps in response to the phishing attempt. The company secured the three affected employee email boxes and is working closely with law enforcement to ensure the

incident is properly addressed. Celink also implemented heightened security measures for the affected customers.

Celink is implementing additional security measures designed to prevent future incidents and to protect the privacy of customers. These measures include implementing a dual-factor authentication system for access to Celink employees' email boxes and enhancing the company's email spam filters.

As a further precaution, Celink is in the process of engaging the services of a credit monitoring service to provide credit monitoring to affected customers, free of charge, for 18 months. Customers will be provided with written instructions as to how to access the credit monitoring service in the letters that they will receive. Customers will not be asked or required to waive any right of private action as a condition of accepting the credit monitoring services described above. Customers will also be given the name and phone number of a person at Celink to contact in the event that they have questions.

Thank you for your attention to this matter. For further information or assistance, please contact Seph McNamara, First Vice President and Associate General Counsel, at Seph.McNamara@Celink.com.

Sincerely,

Rex Lamb
Compliance Officer
512-691-1120

Enclosure: Template Consumer Notice Letter

Celink™
Your Reverse Mortgage Ally

[DATE]

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]

Re: Notice of Data Security Incident

Dear [INDIVIDUAL NAME]:

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that involves your personal information.

Who We Are

Celink is a Michigan-based servicer and subservicer of reverse mortgage loans. Celink is providing you this notice on its own behalf and as subservicer for [NAME OF CLIENT SERVICER]

What Happened

On June 3, 2019, Celink was the target of a phishing attempt by an outside party in the form of an email to Celink employees that appeared to be from a company in our industry. The email contained a link that appeared to be for a secure, encrypted message. When a few employees clicked on the link, the outside party gained access to three employee email boxes. Celink promptly terminated the access and secured these three employee email boxes. Celink also notified the Michigan State Police of the incident. The Michigan State Police is investigating the incident and took steps to prevent further third-party access to the data. At the request of the Michigan State Police, no notifications to affected individuals were made until the Michigan State Police determined that notifications would no longer impede the criminal investigation. Celink is unaware of any instances of identity theft, fraud, or financial loss associated with this incident.

What Information Was Involved

The small quantity of electronic data that could have been accessed included some personal information such as names, addresses, partial Social Security numbers (the last four digits only), and Celink administrative numbers. The data accessed did not include any security codes, access codes, passwords, complete social security numbers, debit or credit card numbers, or bank account numbers.

What We Are Doing

Celink values your privacy and deeply regrets that this incident occurred. Celink has taken several steps in response to the phishing attempt. Celink secured the three affected employee email boxes and is working closely with law enforcement to ensure the incident is properly addressed. Celink also implemented heightened security measures for the affected individuals.

Celink is implementing additional security measures designed to prevent future incidents and to protect the privacy of customers. These measures include implementing a dual-factor authentication system for access to Celink employees' email boxes and enhancing the company's email spam filters.

As an added precaution, we have arranged to provide you with a credit monitoring service for 18 months at no cost to you. [INSTRUCTIONS ON HOW TO ACCESS]

What You Can Do

There are steps you can take to protect yourself, such as placing a freeze on your credit report or contacting the appropriate authorities if you believe you have been the victim of identity theft. The enclosed "STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION" describes some of these steps. Of course, it is always important that you remain vigilant by reviewing your account statements and monitoring free credit reports for signs of fraud.

For More Information

For further information and assistance, please contact William Miller, Vice President, Celink, at 866-508-4494 between 9:00 a.m.- 4:00 p.m. CT daily.

Sincerely,

Rex Lamb
Compliance Officer

Enclosure: Steps You Can Take To Further Protect Your Information

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely for the next 12 to 24 months. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission ("FTC").

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Contact information for the FTC for the purpose of filing a complaint is provided below:

Federal Trade Commission
1-877-ID-THEFT (877-438-4338)
www.ftc.gov/idtheft
600 Pennsylvania Avenue, NW
Washington, DC 20580

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alert

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http:// www.annualcreditreport.com.

Credit Report Monitoring

In addition, Celink has arranged with [SERVICE PROVIDER] to provide you with credit monitoring for 18 months, at no cost to you. The credit monitoring package provides you with the following benefits: [SUMMARY OF BENEFITS]

To take advantage of this offer, you must enroll within 90 days from receipt of this letter. [ENROLLMENT INSTRUCTIONS]

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources on Identity Theft

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).