Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

January 14, 2021

Via Email: *DOJ-CPB@doj.nh.gov; Attorneygeneral@doj.nh.gov*

Attorney General Gordon McDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

To Whom It May Concern:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents SN Servicing Corporation ("SN"), a subsidiary of Security National Master Holding Company, LLC, with respect to a recent data security incident described in more detail below. SN takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the Security Incident

SN experienced a ransomware incident (hereinafter, the "Incident") first discovered by SN on or about October 15, 2020. In response, SN immediately notified the Federal Bureau of Investigation ("FBI") and quickly engaged a third-party cybersecurity forensics investigator to investigate and contain the Incident.

On or about November 24, 2020, the third-party cybersecurity forensics investigator hired by SN to review the Incident concluded the forensics investigation (hereinafter, the "Investigation"). Based on the results of the Investigation, SN learned that a ransomware threat actor group known as "Mount Locker" (hereinafter, the "Threat Actor") was responsible for deploying ransomware onto SN's environment on or about October 15, 2020. According to the results of the Investigation, the Threat Actor successfully exfiltrated (acquired) a number of digital files maintained by SN during a period of time that began or about October 14, 2020 and ended on or about October 15, 2020.

SN has recently hired a third-party e-discovery vendor to conduct a "data mining" review of the documents that were identified to have been exfiltrated by the Threat Actor to determine whether personally identifiable information ("PII") or non-public personal information ("NPI") is contained therein.

2. Number of New Hampshire Residents Affected

As discussed above, SN is actively reviewing the documents that were determined to have been compromised with the assistance of a third-party e-discovery vendor. However, upon preliminary review,

SN has already discovered that the Incident resulted in the unauthorized exposure of information[1] pertaining to a population (hereinafter, the "affected population") of at least eight (8) residents of the State of New Hampshire. So far, SN has determined that this information was largely limited to March 2018 Billing Statements and fee notices which may include, but is potentially not limited to: borrower names, addresses, loan numbers, balance information and billing information such as charges assessed, owed and/or paid.

3. Steps Taken

In addition to hiring multiple third-party vendors to assist with investigating the Incident, SN will mail incident notification letters addressed to the affected population on January 15, 2021, via First Class Mail. A copy of the incident notification letter is enclosed as **Exhibit A**. Additionally, to prevent a similar event from occurring again in the future, SN is taking action to bolster its cybersecurity posture including, and potentially not limited to:

- Replacing email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence (AI) to detect and block known and newly introduced malware;
- Blocking all inbound and outbound internet, email, and network traffic to foreign countries; and
- Upgrading infrastructure to improve backup and recovery efforts if needed.

Please note that, as of this writing, SN has not received any reports of fraud or identity theft related to this matter. As discussed above, SN's review of the Incident remains ongoing. Should SN determine that the nonpublic personal information ("NPI") and/or personally identifiable information ("PII") of any additional residents of the State of New Hampshire was impacted as a result of the Incident, SN will update your Office promptly.

SN remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@wilsonelser.com or (312) 821-6164.

Very truly yours,

WILSON ELSER MOSKOWITZ EDELMAN AND DICKER LLP

Anjali C. Das

[1] The exact elements of personal information that were exposed varied per data subject.

EXHIBIT A

SERVICING CORPORATION
323 5TH STREET
EUREKA CA 95501

(800) 603-0836
Para Español, Ext. 2660 o 2643
8:00 a.m. – 5:00 p.m. Pacific Time
Main Office NMLS #5985
Branch Office NMLS #9785

[redacted]

LoanID: [redacted]

[redacted]

The following disclosures are provided for informational purposes and should not be considered as an attempt to collect a debt. If you have received a discharge in bankruptcy and this debt was not reaffirmed, this correspondence is not an attempt to collect the debt as a personal liability.

NOTICE OF DATA BREACH

Dear Borrower:

We are writing to inform you of a data security incident affecting SN Servicing Corporation ("SN") that has resulted in the exposure of some of your personal information. This letter contains information about the incident, steps we are taking to address the matter, and steps you can take to protect your personal information. Although we are not aware of the misuse of any of your information, we sincerely apologize for any inconvenience this incident may cause.

What Happened

On or about October 15, 2020, SN experienced a cybersecurity attack known as "ransomware." During a ransomware attack, cyber attackers attempt to digitally lock a company's data and hold it for ransom. In response to the Incident, SN immediately locked down affected systems and engaged a third-party team of forensics experts to determine the potential impact to our borrowers. In addition, SN immediately notified the appropriate authorities of the Incident.

What Information Was Involved

Based on the preliminary results of the investigation, we determined that some of your information has been acquired by the individual(s) responsible for the incident. At this time, it is believed that none of the information that was compromised included credit card information, or banking account information from checks or related materials. The information compromised was largely limited to March 2018 Billing Statements and fee notices which may include, but is potentially not limited to: your name, address, loan numbers, balance information and billing information such as charges assessed, owed and/or paid.

We are still in the process of conducting a comprehensive investigation of this incident and you will be notified in the event we discover that any additional nonpublic personal information ("NPI") or personally identifiable information ("PII") pertaining to you was exposed. That being said, we felt it necessary to notify you of this event. As discussed above, we have no evidence at this time that any of your information has been misused.

What We Are Doing

SN is bolstering its cybersecurity posture by:

- Replacing email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence (AI) to detect and block known and newly introduced malware.
- Blocking all inbound and outbound internet, email, and network traffic to foreign countries.
- Upgrading infrastructure to improve backup and recovery efforts if needed.

What You Can Do

Out of an abundance of caution, we are encouraging you to remain vigilant over next twelve (12) to twenty-four (24) months, review your account statements and immediately report any suspicious activity. We also recommend that you regularly obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions, if any, deleted. If you believe you have been the victim of identity theft or need additional guidance with respect to identify theft, we encourage you contact the Federal Trade Commission ("FTC"). The FTC can be reached via telephone at 1-877-IDTHEFT (438-4338) or online at http://www.consumer.gov/idtheft. Further, we encourage you to review the enclosed list of recommended steps you can take to protect yourself.

For Additional Information

Again, we sincerely apologize for any inconvenience caused by this Incident. We also want to assure you are committed to full transparency about the Incident. If you have any questions, please contact us at 1-800-603-0836 between the hours of 08:00pst and 18:00pst.

Sincerely,

SN Servicing Corporation

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:
You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.
Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

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

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.