



RECEIVED

JUL 26 2021

CONSUMER PROTECTION
DIVISION

Notice of Cybersecurity Incident

July 15, 2021

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

Via First-Class Mail

**Attorney General Lawrence Wasden
Office of the Attorney General
700 W. Jefferson Street, Suite 210
P.O. Box 83720
Boise, Idaho 83720-0010**

Dear Attorney General Wasden,

We represent the Security National Master Holding family of organizations, including SN Servicing Corporation (collectively, "SN"). This notice is in regard to a cybersecurity incident (hereafter, the "Incident") that occurred at SN. SN takes the privacy and security of the information in its control seriously, and took steps to mitigate the effects of the incident.

Nature of the Incident

On or about October 15, 2020, SN discovered unauthorized access to its network. Upon discovery, SN immediately terminated the access and initiated an investigation to determine the nature and scope of the Incident. This investigation concluded on or about November 24, 2020. Based on the results of the investigation, it was determined that an unauthorized party may have been able to access sensitive personal information for some of its borrowers. SN reviewed its internal documentation system, and was able to notify the first segment of individuals on or about January 15, 2021.

SN subsequently launched a supplemental investigation to determine whether additional individuals may have been impacted by utilizing a data mining vendor. We received the preliminary results of this investigation on or about April 22, 2021. Based on these results, SN engaged in a substantial data validation process to verify the accuracy of the data. Immediately after concluding its validation procedures, SN procured credit monitoring for affected individuals and drafted notices to individuals, consumer credit reporting agencies, and state regulators as appropriate.

What Information Was Involved

SN has no reason to believe that any individuals' information has been misused as a result of this incident, and notified all individuals out of abundance of caution and for purposes of full transparency. Based on the investigation, the unauthorized party may have had access to one or more of the following data elements: name, contact information, date of birth, social security number, and loan/borrower information. Please note that not every data element was present for every individual.

Steps Taken

SN engaged a specialized cybersecurity firm to conduct an investigation of the Incident. Since the Incident, SN has continued to strengthen their security posture. Additionally, an incident notification letter has been

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Allanta • Austin • Baltimore • Beaurmont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

sent out to individuals, and SN has also made complimentary credit monitoring and identity theft protection services available for all affected individuals. A copy of the notice letter is enclosed as **Exhibit A**.

Contact Information

SN remains dedicated to protecting the sensitive information in 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 & Dicker LLP



Anjali C. Das

Enclosure

Exhibit A

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

Notice of Cybersecurity Incident

[Date], 2021

Via Physical Mail

<Individual>
<Address 1>
<Address 2>
<City><State><Zip>

Dear <Individual>,

Out of an abundance of caution, we are writing to inform you of a cybersecurity incident which affected the SN Servicing Corporation (“SN”). The cybersecurity incident may have resulted in the potential compromise of some of your data. This letter contains information about the incident and information about how to protect your personal information going forward. SN considers the protection of sensitive information a top priority, and sincerely apologizes for any inconvenience as a result of the incident.

What Happened

On or about October 15, 2020, SN discovered unauthorized access to its network. Upon discovery, SN immediately terminated the access and retained a specialized cybersecurity forensic team to conduct an investigation to determine the nature and scope of the Incident. The forensics team first identified the name and locations of files that were exfiltrated from the firewall records. This investigation concluded on or about November 24, 2020. Based on the results of the investigation, it was determined that an unauthorized party may have been able to access sensitive personal information for some of our borrowers.

SN was able to quickly identify a subset of documents which were believed to contain sensitive information for some borrowers. In the interest of notifying the borrowers as quickly as possible, a preliminary notice was provided for that collection of documents as quickly as possible. A data mining vendor was then hired to review the remaining documents to identify any additional individuals that may have been affected and what data may have been exposed. The data mining vendor provided its results on or about April 27, 2021.

SN engaged in a substantial data validation process to verify the accuracy of the data and reconcile to internal records. Immediately after concluding its validation procedures, SN procured credit monitoring for affected individuals and drafted notices to individuals, consumer credit reporting agencies, and state regulators as appropriate.

What Information Was Involved

While we have no reason to believe that your information has been misused as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the unauthorized party may have had access to one or more of the following data elements: name, contact information, date of birth, social security number, and loan/borrower information. Please note that not every data element was present for every individual. While we appreciate that the incident may be concerning, please note that SN is not aware of any instances of misuse of sensitive data.

What We Are Doing

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Allanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

SN engaged a specialized cybersecurity firm to conduct an investigation of the incident. Since the incident, SN has continued to strengthen its security posture. Additionally, we have also obtained complimentary credit monitoring for all affected individuals. We encourage you to take advantage of the complimentary credit monitoring services. We are making these services available to you at no cost; however, you will need to enroll yourself in these services.

What You Can Do

We recommend that you continue to remain vigilant in monitoring your personal information. The easiest way to do this is to take advantage of the complimentary credit monitoring and identity theft services we are offering to you. Details regarding these services are included in a separate attachment to this letter. To reiterate, we are making these services available to you at no cost; however, you will need to enroll yourself in these services.

There are additional steps you can take to protect yourself which are contained in the supplement to this letter titled "*Additional Important Information.*"

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause. If you have any questions, please do not hesitate to call [PHONE NUMBER] Monday through Friday, between 8:00 AM and 5:00 PM Central time.

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:

Fair Credit Reporting Act: You are also advised that you may have additional rights under the federal Fair Credit Reporting Act.

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

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

(<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
(800)-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
(888)-397-3742

www.experian.com/freeze

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
(800)-680-7289

freeze.transunion.com

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

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Allanta • Austin • Baltimore • Beadment • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com