[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

From: Leray.Jackson@wellsfargo.com <Leray.Jackson@wellsfargo.com>
Sent: Thursday, February 25, 2021 5:27 PM
To: DOJ: Attorney General <attorneygeneral@doj.nh.gov>
Cc: cdtlegal@wellsfargo.com; Wesley.T.Glosser@wellsfargo.com; CDRNIV@wellsfargo.com
Subject: Notice of Data Security Breach - Wells Fargo Bank, N.A.

EXTERNAL: Do not open attachments or click on links unless you recognize and trust the sender.

VIA E-MAIL

New Hampshire Department of Justice

Gordon J. MacDonald, Attorney General
33 Capital Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Mr. MacDonald:

This notice is being provided in compliance with New Hampshire N.H. Rev. Stat. §§ 359-C:19 et seq. Requested data security incident information as follows:

- Name and contact information of person reporting the breach.
  Ray Jackson, Business Support Consultant
  Wells Fargo Bank, N.A. | 2850 S. Price Rd, Chandler, AZ
  MAC: S3930 – 01G
  Cell: 480-572-9367

- Name and address of business that experienced the breach, and the type of business.
  Wells Fargo Clearing Services, LLC.
  One North Jefferson
  St. Louis, MO 63103

- A general description of the breach, including the date(s) of the breach, when and how the breach was discovered, and any remedial steps taken in response to the breach.
  On February 8, 2021, a Wells Fargo Clearing Services, LLC employee inadvertently emailed a brokerage Account Agreement containing customer personal information (name, address, social security number, brokerage account number) to an unintended recipient. The unintended recipient has been contacted but email deletion has not been confirmed. The activity impacted one (1) resident of New Hampshire. Wells Fargo is continuing to review its security measures to help mitigate future risk and is offering the impacted resident two years of complimentary credit monitoring.

- The number of individuals affected by the breach.
  The activity impacted one (1) resident of New Hampshire

- A detailed list of the categories of personal information subject of the breach.
  Data elements compromised: name, address, social security number, and brokerage account number

- The date notification will be sent to the affected individual.
  February 26, 2021

- A template copy of the notification sent to the affected individual.
  *****Please See Attached***

- Whether credit monitoring or identity theft protection services has been or will be offered to affected individuals, as well as a description and length of such services.*

  Wells Fargo is continuing to review its security measures to help mitigate future risk and is offering the impacted resident two years (24 months) of complimentary credit monitoring.

- Whether the notification was delayed due to a law enforcement investigation (if applicable).

  N/A

Please contact me with any questions or if I may assist further in any way with the foregoing.

Thank you!

Ray Jackson

AVP | Business Support Consultant

ENTERPRISE OPERATIONAL SUPPORT | COMPROMISED DATA REGULATORY NOTIFICATIONS & INCIDENT VALIDATION

Wells Fargo Bank, N.A. | Chandler, AZ

MAC: S3930 – 01G

Tel: 480-887-3608

Cell: 480-572-9367

leray.jackson@wellsfargo.com

-

Wells Fargo Bank, N.A.
MAC D1118-02U
P.O. Box 71117, 2nd Floor
Charlotte, NC 28272-1117

WELLS FARGO

[redacted]

[redacted]

Subject: **Notice of Data Breach**

Dear [redacted]:

We are writing to inform you of an incident that may affect the security of your personal information. Protecting our customers' information is a top priority. We apologize for any inconvenience or concerns this may cause. This letter provides information about the incident and resources available to help you protect your information.

What happened?
On February 12, 2021, we learned that on February 8, 2021, a new account package containing your personal information was inadvertently emailed to an unintended recipient. We attempted to contact the recipient but have not been able to confirm that the email was deleted.

What information was involved?
The personal information involved included your name, address, account number and social security number.

What we are doing
We are continually review our security measures to reduce the likelihood of this happening in the future. We are offering you a complimentary two-year subscription to Experian IdentityWorks℠. This product provides you with identity detection that includes daily monitoring of your credit reports from the three national credit reporting companies (Experian®, Equifax® and TransUnion®), internet surveillance, and resolution of identity theft.

To accept this offer, please activate your subscription within 60 days of the date printed on this letter. Enroll online at www.experianidworks.com/3bplus or call 1-877-890-9332, Monday through Friday, 8:00 a.m. - 8:00 p.m. Central Time and Saturday/Sunday, 10:00 a.m. - 7:00 p.m. Central Time. By law, we cannot enroll for you.

You will be asked to provide the following information for enrollment:
- Activation Code: [redacted]
- Engagement Number: [redacted]
- Your social security number, email address, mailing address, phone number, and date of birth

At the end of your free subscription, these services will automatically be canceled and you will not be billed. Please see additional details enclosed.

What you can do
In addition to enrolling in the Experian IdentityWorks[SM] credit monitoring service, we encourage you to read and follow the enclosed *Tips to Protect Your Personal Information*.

For more information
We are here to help. If you have questions, please call Adam Litzau, Financial Advisor, at 1-866-636-8339, extension 725343, Monday through Friday, 8:00 a.m. to 4:30 p.m. Central Time. For customers with hearing or speech disabilities, we accept telecommunications relay service calls.

Thank you. We appreciate your business.

Sincerely,

Kombiz Momtaz

Kombiz Momtaz
Digital Advice Manager

Enclosure

[redacted]
20210101

Tips to Protect Your Personal Information

Credit Monitoring

Take advantage of the Experian IdentityWorks℠ subscription we are offering you.

Features of Experian IdentityWorks℠ include:

- ✓ **Experian® credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- ✓ **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- ✓ **Credit Monitoring:** Actively monitors Experian®, Equifax® and TransUnion® files for indicators of fraud.
- ✓ **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers. **
- ✓ **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- ✓ **Experian's IdentityWorks ExtendCARE™**: You receive the same high level of Identity Restoration support even after your Experian IdentityWorks℠ membership has expired.

**Offline members will be eligible to call for additional reports quarterly after enrolling.*
*** Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage.*

Protecting Your Accounts

Monitor your account statements often (even daily in online banking) to review all charges and transactions. Contact us immediately at 1-800-TO-WELLS (1-800-869-3557) 24 hours a day, and 7 days a week, if you see discrepancies or unauthorized activity on your Wells Fargo accounts. We will carefully review them for reimbursement in accordance with our policies.

If available, consider placing password protection on your Wells Fargo accounts, and do not use any part of your social security number as the username or password. To find out if password protection is available for your accounts, visit any Wells Fargo branch. Or we can help you close these accounts and transfer the money to new accounts. For this option, please call us at 1-800-TO-WELLS (1-800-869-3557), 24 hours a day, and 7 days a week, or visit any Wells Fargo branch.

If your user name or email address, with a password or security question and answer that would permit access to an online account were involved, promptly change you user name or password and security question or answer, as applicable, or take other appropriate steps to protect online accounts for which you use the same user name or email address and password or security question and answer.

Do not write down or share your Personal Identification Number (PIN) number or passwords with anyone.

If you receive suspicious emails that claim to be from Wells Fargo, forward them toreportphish@wellsfargo.com and then delete them.

If you have accounts at other financial institutions, please notify them and they can advise you on additional steps to take.

For more tips on how to protect your Wells Fargo accounts, please visit www.wellsfargo.com/privacy_security

Protecting Your Identity

Check your credit report to ensure all your information is correct. You can obtain a free credit report from each of the three major credit bureaus every 12 months by visiting **www.annualcreditreport.com** or calling 1-877-322-8228. Credit bureau contact details are provided below.

Equifax®:
1-800-525-6285 or
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian®:
1-888-397-3742 or
www.experian.com
P.O. Box 9532
Allen, TX 75013

TransUnion®:
1-800-680-7289 or
www.transunion.com
P.O. Box 6790
Fullerton, CA 92634

You also may want to consider placing a freeze on your credit file. A credit freeze means potential creditors cannot get your credit report and makes it less likely that an identity thief can open new accounts in your name. To place a freeze on your credit you can contact the nationwide credit bureaus. You can freeze your credit for free, but you'll need to supply your name, address, date of birth, social security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. To lift the freeze, you will need to contact the credit bureaus again.

Place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus listed to the left. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.
This provides a significant layer of protection; however, it may limit your ability to get "instant credit" such as the offers often available at retail branches.

If you believe you are a victim of identity theft, report it to your local law enforcement agency and to the Federal Trade Commission (FTC) or your state Attorney General.
FTC Consumer Response Center
600 Pennsylvania Avenue, NW, H-130
Washington, DC 20580
1-877-438-4338
www.identitytheft.gov

Contact information for the state's Attorney General's offices can be found at **www.naag.org**.

Contact information for the Attorney General's office in the following states:

For Maryland:
200 St. Paul Place
Baltimore, MD 21202-2202
1-888-743-0023
www.marylandattorneygeneral.gov

For North Carolina:
Dept. of Justice, P.O. Box 629
Raleigh, NC 27602-0629
919-716-6400
www.ncdoj.gov

For Rhode Island:
150 S. Main St.
Providence, RI 02903
401-274-4400
www.riag.ri.gov