

From: [Layman, James](#)
To: [REDACTED]
Cc: [Mishaan, Jessica](#)
Subject: Vermont Public Records Request Response
Date: Thursday, October 31, 2024 11:51:52 AM
Attachments: [2024-10-31 Wells Fargo Breach PRA Response - Harvey.pdf](#)
[Webform submission from VERMONT STATE SECURITY BREACH REPORTING FORM.pdf](#)
[2024-09-19 Wells Fargo Bank Data Breach Notice to Consumers.pdf](#)
[Notice of Data Breach - Wells Fargo Clearing Services, LLC \(Vermont\).pdf](#)

Dear Mr. Harvey,

In response to your public records request, please find enclosed a letter and three responsive documents. Please let me know if you have any questions.

Sincerely,

James Layman
Assistant Attorney General
Vermont Office of the Attorney General
Environmental and Public Protection Division
109 State Street
Montpelier, VT 05609-1001
802.828.2315
james.layman@vermont.gov



STATE OF VERMONT
OFFICE OF THE ATTORNEY GENERAL
109 STATE STREET
MONTPELIER, VT
05609-1001

October 31, 2024

Via email to: [REDACTED]

Re: Public Records Request

Dear Mr. Harvey:

I write in response to your Public Records Act request received by the Attorney General's Office on October 30, 2024 in which you requested: "Please provide any and all details that are applicable to my account with Wells Fargo. Any leaked information or fraud?" We understand this as a request for any documents related to a Wells Fargo data breach that was reported in September 2024.

In response to your request, we have identified four documents in our records related to a security breach reported by Wells Fargo. I have enclosed with this email PDFs of three of those documents, all of which are security breach notices provided to our office by representatives of Wells Fargo in September 2024.

I have withheld one document pursuant to the Vermont Public Records Act's exemption for records "that by law are designated confidential," 1 V.S.A. § 317(c)(1), as the withheld document is a Preliminary Notice of a data breach, dated September 19, 2024. Preliminary Notices are confidential as a matter of law pursuant to 9 V.S.A. § 2435 (b)(3)(B)(iv). Note that, although this document has been withheld due to legal requirements, it does not contain any information that is not already provided in the other documents being produced to you today.

To the extent you feel information has been withheld in error, you may appeal to the Deputy Attorney General, Robert McDougall. Such appeal should be in writing to: Attorney General's Office, Attn: Robert McDougall, 109 State Street, Montpelier, VT 05609-1001 or ago.publicrecordsrequests@vermont.gov.

Sincerely,

A handwritten signature in cursive script that reads "James Layman".

James Layman
Assistant Attorney General
Environmental and Public Protection Division



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

August XX, 2024

Name
Address
City, ST ZIP

Notice of Data Breach

Dear Name,

We are following up on the incident that occurred that affects 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?

We recently learned that a former employee accessed, and in some cases used, customer information for fraudulent purposes. Upon discovery, we initiated an investigation and reported the matter to law enforcement. In July 2024, we discovered that your personal information was accessed. Below is more information on the event, and an offer of identity theft protection services.

What information was involved?

The personal information accessed between May 2022 and March 2023 may have included your name, address, date of birth, phone number, email address, social security number, driver's license number, bank account number(s), credit/debit card number(s), brokerage account number(s), and/or loan/line of credit number(s).

What we are doing

We take our responsibility to safeguard your information very seriously. We promptly responded to this incident and have been working diligently to notify you and to assist you in protecting your information. We are continually working to improve how we protect your information. We are taking measures to monitor your account(s) for suspicious events or changes and 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 IdentityWorksSM. This product provides you with identity theft detection services that include daily monitoring of your credit reports from the three national credit reporting companies (Experian[®], Equifax[®] and TransUnion[®]), internet surveillance to monitor activity associated with your identity, and full-service identity restoration in the event of identity theft.

To accept this offer, please activate your subscription within 60 days of the date printed on this letter.
You may activate this offer:

- online at <https://www.experianidworks.com/3bplus>; or
- by calling **1-877-890-9332**, Monday - Friday, from 8:00 a.m. to 8:00 p.m. Central Time and Saturday - Sunday, from 10:00 a.m. to 7:00 p.m. Central Time.

When enrolling, the member will need to provide to Experian information such as name, contact information, Social Security Number (SSN), date of birth, and the unique codes provided below. By law, we cannot enroll for you.

Your Activation Code: **CMCode**
Engagement Number: **XXXXXXXX**

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 IdentityWorksSM credit monitoring service, we encourage you to read and follow the enclosed *Tips to protect your personal information*.

For more information

We're here to help. If you have questions or other requests such as requesting a larger font or translation, please call our Customer Advocacy Support Team at **1-866-885-3802** and refer to this letter (there is no charge for these services). Representatives are available Monday - Friday, from 9:00 a.m. to 4:00 p.m. Pacific Time. Language assistance services are available. If you have hearing or speech difficulties, we accept relay service calls.

Thank you. We appreciate your business.

Sincerely,

Stephanie Walzberg
Executive Director
Compromised Data

Enclosure

Tips to protect your personal information

Credit monitoring

Take advantage of the Experian IdentityWorksSM subscription we are offering you. Features of Experian IdentityWorksSM 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 ExtendCARETM:** You receive the same high level of Identity Restoration support even after your Experian IdentityWorksSM membership has expired.

**Offline members will be eligible to call for additional reports quarterly after enrolling. The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

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

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. In some states, you may be entitled to file or obtain a police report, if such a report exists.

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

From: [Jackson, Leray](#)
To: [AGO - Security Breach](#)
Cc: [CDRNIV](#)
Subject: Notice of Data Breach - Wells Fargo Clearing Services, LLC (Vermont)
Date: Wednesday, September 18, 2024 12:59:13 PM
Attachments: [image001.png](#)

Some people who received this message don't often get email from leray.jackson@wellsfargo.com. [Learn why this is important](#)

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

VIA EMAIL SUBMISSION

Vermont Attorney General's Office
Attn: Ryan Kriger, Assistant Attorney General
109 State Street
Montpelier, VT 05609
ago.securitybreach@state.vt.us

Mr. Kriger:

This notice is being provided in compliance with [9 V.S.A. §§ 2430, 2435](#). Requested data security incident information as follows:

- **Name and contact information of person reporting the data security breach.**
Ray Jackson, Senior Lead Business Execution Consultant
Wells Fargo Bank, N.A. | 2700 S. Price Rd, Chandler, AZ
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.**
A Wells Fargo investigation recently confirmed that the personal information of multiple Wells Fargo Bank, N.A. and Wells Fargo Clearing Services, LLC customers was accessed, and sometimes misused, by a Wells Fargo employee. The personal information impacted may have included a combination of the customers' name, account number, brokerage account number, full Social Security number, Driver License number, date of birth, phone number and address. At this time, Wells Fargo has determined that the personal information of two (2) residents of Vermont may have been affected. The investigation, however, is continuing, and Wells Fargo will notify any other individuals whose personal information it determines may have been affected.

The individual was employed with Wells Fargo between May 2022 and March 2023 as a Securities Operations Representative with Wells Fargo Clearing Services, LLC. During this time, the employee accessed customer bank and brokerage accounts without a business need, made unauthorized account profile changes, and completed or attempted to complete fraudulent transactions on the accounts. This activity has been confirmed by Wells Fargo's investigations and monitoring teams.

Wells Fargo will reimburse impacted customers for any fraudulent charges and related fees as appropriate, review and close impacted accounts as appropriate, open new accounts upon request, implement enhanced fraud monitoring processes for the customers involved, and notify all customers regarding this incident who may have been affected and provide them with an offer of

two years of complimentary credit monitoring. The employee no longer works for Wells Fargo and law enforcement has been engaged.

- **The number of Vermont residents notified regarding this incident.**
Wells Fargo will notify two (2) residents of Vermont
- **A detailed list of the categories of personal information subject to the breach.**
The personal information impacted may have included a combination of the customers' name, account number, brokerage account number, full Social Security number, Driver License number, date of birth, phone number and address
- **The anticipated date notification will be sent to the affected individuals.**
September 18, 2024 via US Mail
- **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.**
W and the affected Vermont residents will be offered two years of complimentary credit monitoring.
- **Whether the notification was delayed due to a law enforcement investigation (if applicable).**
No

Please contact me with any questions.

Thank you,

Ray Jackson

Senior Lead Business Execution Consultant | Executive Director
Regulatory Operations | Global Privacy Utility

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

Cell: 480-572-9367

leray.jackson@wellsfargo.com



This message may contain confidential and/or privileged information. If you are not the addressee or authorized to receive this for the addressee, you must not use, copy, disclose, or take any action based on this message or any information herein. If you have received this message in error, please advise the sender immediately by reply e-mail and delete this message. Thank you for your cooperation.

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: leray.jackson@wellsfargo.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Thursday, September 19, 2024 9:59:51 AM

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

Submitted on Thu, 09/19/2024 - 13:59

Submitted by: Anonymous

Submitted values are:

Name

Wells Fargo Bank, N.A.

Street Address

420 Montgomery St.
San Francisco, California. 94104

Name

Ray Jackson

Title

Senior Lead Business Execution Consultant

Dated

2024-09-19

Telephone

[4805729367](tel:4805729367)

Email

leray.jackson@wellsfargo.com

Relationship to Entity whose information was compromised

Current employee

(please select one)

Financial Services

Total (Including VT residents)

607

Total VT Residents

2

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2023-03-27

Breach Discovered

2024-07-22

Consumer Notification(s)

2024-09-19

(select all that apply)

Insider wrongdoing

(select all that apply)

Social Security Number, Driver's license number or non-driver identificaiton card number, Financial account number or credit or debit card number

(select all that apply)

Written

Has anything been offered?

Yes

Duration

24 months

Provider

Experian IdentityWorks

Brief Description of Service

Complimentary credit monitoring

Please attach Form of Consumer Notice

[803385_FINAL.pdf](#) (102.94 KB)