



3701 Wilshire Blvd., Suite 900, Los Angeles, CA 90010
Tel: (213) 210-2000 | Fax: (213) 355-8850

October 7, 2021

VIA EMAIL

NH Department of Justice
33 Capitol Street
Concord, NH 03301
Email: attorneygeneral@doj.nh.gov

Re: Notification of Cybersecurity Incident

Dear Attorney General Formella:

Pursuant to N.H. Rev. Stat. §§ 359-C:19, C:20, C:21, I am writing to notify you of a cybersecurity incident at Pacific City Bank (“PCB”) involving two New Hampshire residents. PCB is an FDIC-insured and CA-State chartered bank, with its principal headquarters located at 3701 Wilshire Boulevard, Suite 900, Los Angeles, California 90010.

Nature of the Cybersecurity Incident

On August 30, 2021, PCB identified unusual activity on its network. PCB responded promptly to disable the activity, investigate its source and monitor PCB’s network. PCB subsequently became aware of claims that it had been the target of a ransomware attack. On September 7, 2021, PCB determined that an external actor had illegally accessed and/or acquired certain data on its network. PCB has been working with third-party forensic investigators to understand the nature and scope of the incident and determine what information may have been accessed and/or acquired and who may have been impacted. The investigation revealed that this incident impacted certain files containing certain PCB customer information. Some of these files contained documents related to loan applications, such as tax returns, Form W-2 information of their employees, and payroll records.

Affected New Hampshire Residents

The two New Hampshire residents affected by this breach have been notified by U.S. Mail. A sample copy of the notice to New Hampshire residents is enclosed with this letter.

Steps PCB Has Taken

The privacy and security of customer information is of the utmost importance to PCB, and we take this incident very seriously. As part of our ongoing commitment to ensuring the security of information in our care, we have reported this incident to appropriate law enforcement authorities. We also are continuing our investigation into this incident and are working to review our existing policies and procedures, including our information security plan, to evaluate measures and safeguards to protect against this type of incident in the future. Although we are unaware of any misuse of impacted

information as a result of this incident, we are offering one year of Equifax Complete Premier credit and identity monitoring service at no cost to these New Hampshire consumers.

Contact Information

If you have questions about this cybersecurity incident and/or PCB's response, please do not hesitate to contact the undersigned.

Sincerely,

A handwritten signature in black ink, appearing to read 'Andrew Chung', enclosed within a large, horizontal oval stroke.

Andrew Chung
Executive Vice President & Chief Risk Officer
Pacific City Bank

Enclosure



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

Pacific City Bank (“PCB”) takes the privacy and security of information entrusted to us very seriously. We are writing to notify you of a cybersecurity incident that may impact the security of your personal information. We apologize for any concern this may cause and assure you that we are giving this matter our urgent attention. This letter provides information about the incident and about steps we are taking to help you protect your personal information.

What Happened: On August 30, 2021, PCB identified unusual activity on its network. PCB responded promptly to disable the activity, investigate its source and monitor PCB’s network. PCB subsequently became aware of claims that it had been the target of a ransomware attack. On September 7, 2021, PCB determined that an external actor had illegally accessed and/or acquired certain data on its network. PCB has been working with third-party forensic investigators to understand the nature and scope of the incident and determine what information may have been accessed and/or acquired and who may have been impacted.

The investigation revealed that this incident impacted certain files containing certain PCB customer information. Some of these files contained documents related to loan applications, such as tax returns, Form W-2 information of their employees, and payroll records. Your information was included as part of the supporting documentation of your employer’s loan application.

What Information Was Involved: The personal information impacted may include some or all of the following personal information: your name, address, Social Security Number, wage and/or tax information. Please note that the exact nature and extent of personal information impacted may vary by individual.

What We Are Doing: The privacy and security of information entrusted to us is of the utmost importance to PCB, and we take this incident very seriously. We have reported this incident to the appropriate law enforcement authorities. As part of our ongoing commitment to ensuring the security of information in our care, we have conducted a thorough investigation into this incident and are continuing to monitor our systems’ security. In addition, we are working to review our existing policies and procedures, including our information security plan, to evaluate additional measures and safeguards to protect against this type of incident in the future.

What You Can Do: It is always important to remain vigilant and monitor your financial account statements and credit reports for signs of fraud. In addition, PCB is offering you one year of **free** Equifax Complete Premier credit monitoring and identity theft protection. You will not be billed for this service. Instructions for enrolling in the Equifax Complete Premier program are enclosed with this letter. If you are under the age of 18, you will need to call 855-675-2855 to receive a code that allows you to enroll in the Equifax credit monitoring and identity theft protection service for individuals under age 18. The enclosed material also provides important information about additional steps you can take to protect your information.

Security Freeze Information: You can request a “Security Freeze” on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze

PO Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-685-1111

Experian Security Freeze

PO Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze

PO Box 2000
Chester, PA 19016
<http://transunion.com/freeze>
1-888-909-8872

- Your full name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.)
- Your Social Security Number
- Your date of birth (month, day and year)
- Your complete address including proof of current address, such as a current utility bill, bank or insurance statement or telephone bill
- If you have moved in the past 2 years, give your previous addresses where you have lived for the past 2 years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

Within 5 business days of receiving your request for a security freeze, the consumer credit reporting company will provide you with a personal identification number (PIN) or password to use if you choose to remove the freeze on your consumer credit report or to authorize the release of your consumer credit report to a specific party or for a specified period of time after the freeze is in place.

Other Important Information: If you believe you are the victim of identity theft, you should contact your local law enforcement, the Federal Trade Commission, and/or your state's Attorney General and file a police report.

Please know that the security of your information is of paramount importance to us, and we deeply regret any worry or inconvenience this incident may have caused. If you have additional questions, please call **855-675-2855** between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday.

Sincerely,



Andrew Chung
Executive Vice President & Chief Risk Officer
Pacific City Bank

Enclosures



Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<Activation Code>> then click “Submit” and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click “Continue”.
*If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.
Once you have successfully signed in, you will skip to the Checkout Page in Step 4*
 2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
 3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
 4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page.
Click ‘Sign Me Up’ to finish enrolling.
- You’re done!**
The confirmation page shows your completed enrollment.
Click “View My Product” to access the product features.

¹ The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

² Credit monitoring from Experian and TransUnion will take several days to begin.

³ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded.

⁴ The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

⁵ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

⁶ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.