

RECEIVED

MAY 17 2021

CONSUMER PROTECTION

BakerHostetler

Baker & Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Daniel A. Pepper
direct dial: 215.564.2456
dpepper@bakerlaw.com

May 11, 2021

VIA US MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Sir or Madam:

I am writing on behalf of our client, Oak Valley Community Bank ("Oak Valley"), to notify you of a data security incident. Oak Valley is located at 125 N. Third Avenue, Oakdale, CA 95361.¹

While conducting a routine security review, Oak Valley discovered suspicious activity involving some of its computer systems on February 2, 2021. Upon discovering this activity, Oak Valley immediately secured the systems involved, began an investigation with the assistance of a cybersecurity firm, and notified law enforcement.

Oak Valley's investigation identified unauthorized access to files on one server in its network between February 1, 2021 and February 2, 2021. Oak Valley then conducted a comprehensive review of the affected files on the server. On April 23, 2021, Oak Valley determined that certain of those files contained information regarding current and former bank customers as well as employees of certain businesses that conduct business with Oak Valley. Oak Valley determined the information in the files included the individuals' names and one or more of the following data elements: Social Security number health insurance information, driver's license number, and financial account information.

Beginning today, Oak Valley will mail notification letters to six (6) New Hampshire residents via U.S. First-Class mail. A sample copy of the notice letter is enclosed. Oak Valley is offering the New Hampshire residents two-years of complimentary credit monitoring, fraud

¹ This report does not waive Oak Valley's objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.


Office of the New Hampshire Attorney General
May 11, 2021
Page 2

consultation, and identity theft restoration services through Kroll. Oak Valley has also established a dedicated call center for individuals to call with questions about the incident.

To help prevent something like this from happening in the future, Oak Valley is continuing to regularly audit its systems for potential unauthorized activity and is implementing enhanced network monitoring tools.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,


Daniel A. Pepper
Partner

Enclosure



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>>:

Oak Valley Community Bank is writing to inform you of an incident that involves some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

While conducting a routine security review, we learned of a data security incident involving some of our computer systems. Upon identifying the suspicious activity, we immediately secured the systems involved, commenced an investigation with the assistance of a third-party forensic investigation firm, and notified law enforcement. Through this investigation, we determined that an unauthorized party had accessed a workstation in our network, allowing unauthorized access to files on one file server on February 1, 2021 and February 2, 2021. We undertook a comprehensive review of the data that was accessed to identify individuals whose information was contained in those files. On April 23, 2021, our review confirmed that these files contained information about you, including your <<b2b_text_1(DataElements)>>.

We are committed to protecting the confidentiality and security of the personal information we maintain. We had your information because you are either a customer of Oak Valley Community Bank or your information was included on supporting documentation to establish a loan or other business account. We wanted to notify you of this incident and assure you that we take it very seriously. To help prevent something like this from happening in the future, we have implemented additional policies and electronic security features to enhance our security posture.

We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity you did not authorize, we suggest that you contact the account provider immediately. Additionally, we are offering you a complimentary two-year membership to identity monitoring services at no cost. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. This product helps detect possible misuse of your information and provides you with identity monitoring support. Kroll's identity monitoring services is completely free and activating this service will not hurt your credit score. For more information on Kroll's identity monitoring services, including instructions on how to activate your complimentary two-year membership, as well as some additional steps you can take to help protect yourself, please see the pages that follow this letter.

If you received this letter on behalf of your minor child, please contact Kroll immediately before activating this service, as he/she may be eligible for Minor Identity Monitoring services instead. Identity Restoration specialists are available to help you and your child address credit and non-credit related fraud. You may also contact the Federal Trade Commission and/or the Attorney General's office in your state on their behalf. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. Contact information for the Federal Trade Commission is included on the enclosed under *Additional Steps You Can Take*.

We regret any inconvenience or concern this incident may cause you. Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction. If you have any questions, please call our dedicated call center at **1-855-608-3478**, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some U.S. holidays. Please have your membership number on the following page ready.

Sincerely,

A handwritten signature in black ink, appearing to be 'CMC', written in a cursive style.

Christopher M. Courtney
President & CEO
Oak Valley Community Bank

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years (24 months). Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

To activate:

Visit: <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **August 8, 2021** to activate your identity monitoring services.

Membership Number: <<Member ID>>



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave., Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

District of Columbia: You may contact and obtain information from your attorney general at: *Office of the Attorney General for the District of Columbia*, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us.

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov.

Rhode Island: [This incident involves one \(1\) individual in Rhode Island](#). Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.