

November 1 2022

VIA EMAIL

New Hampshire Attorney General

Re: Arvest Bank – Incident Notification

Dear Sir or Madam:

Buckley LLP represents Arvest Bank (“Arvest”), which is a state-chartered bank. I am writing to notify you of an incident at Overby-Seawell Company (“OSC”), an insurance company that provides property insurance validation for banks and lenders, including Arvest, that may affect the security of personal information of approximately two New Hampshire residents. As a client of OSC, Arvest provided personal information to OSC for OSC to perform such services. Arvest’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Arvest does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On July 11, 2022 Arvest was notified that, on July 5, 2022, OSC discovered suspicious activity on certain computer systems. OSC immediately launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. OSC’s investigation determined that there was unauthorized access to specific OSC servers beginning on May 26, 2022. On July 11, 2022, OSC determined that certain information had been stolen from OSC’s network. OSC undertook a review of the impacted files and later determined that those files contained certain information related to Arvest’s customers. As far as we know this incident was limited solely to OSC, and in particular none of Arvest’s own information systems were affected by this incident. The type of personal information exposed varied but may have included affected residents’ customer name’s, loan amount, loan number, mailing address and insurance policy information.

To date, Arvest is not aware of any identity fraud or improper use of any information as a result of this incident. Nevertheless, out of an abundance of caution, Arvest wanted to inform you (and the affected residents) in New Hampshire of this incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Arvest is providing the affected residents with written notification of this incident commencing on or about October 31, 2022 in substantially the same form as the letter attached hereto. Arvest is offering affected residents complimentary one-year memberships with Arvest’s IDProtect® credit monitoring services. Arvest is also advising affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. Finally, Arvest will provide all affected residents with the contact information for the three primary nationwide consumer reporting agencies as well as the Federal Trade Commission.

New Hampshire Attorney General

November 1, 2022

Page 2

Arvest is committed to maintaining the privacy of customers' personal information and has implemented technical, physical, and administrative safeguards to protect customers' data. Arvest continually evaluates and modifies its data security practices, internal controls, and third-party relationships to enhance the security and privacy of personal information in its possession.

Should you have any questions regarding this notification, please feel free to contact me at 202-349-8089 or alawrence@buckleyfirm.com.

Sincerely,

Amanda Lawrence

Buckley LLP
Partner
2001 M Street NW, Suite 500
Washington, DC 20036
T (202) 349-8089
alawrence@buckleyfirm.com

Notice of Data Breach

Important Information Please Review Carefully

Dear *Customer Name,

Arvest Bank wishes to inform you of a data incident that regretfully resulted in the disclosure of your personal or account information.

What Happened?

We recently received notification from Overby-Seawall Company ("OSC"), our vendor that monitors hazard and flood insurance of a cyber incident that was the result of an unauthorized party gaining access to portions of their systems.

What Information Was Involved?

OSC determined that the following information related to you was present within the impacted files: your name, loan amount, loan number, mailing address, and insurance policy information.

What We Are Doing.

We are requiring the vendor to perform security enhancements. These efforts will include required password changes for Arvest and all other businesses who utilize their service.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident, nor did we delay notice to you because of any law enforcement investigation. However, we wanted to make you aware of the incident, explain the services already available to you, and suggest steps that you should take as well.

What Can You Do.

This letter provides other precautionary measures you can take to protect your information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

In addition, as a result of this incident we are offering you identity theft services through IDProtect® at no charge for one year (through October 1, 2023). Please follow the instructions provided in the enclosed IDProtect® Welcome Kit to take advantage of the breadth of features included in the service, such as receiving alerts and requesting copies of your credit report.

For More Information.

Arvest Bank is committed to protecting our customers' personal information and appreciates your trust and understanding as we provide a secure banking experience. Questions about this incident can be directed to *bank or division name at *(XXX) XXX-XXXX.

Respectfully,

*Associate Name

*Associate Title

Enclosures: IDProtect® Welcome Kit

– OTHER IMPORTANT INFORMATION –

1. **IDProtect® Identity Monitoring**

IDProtect® is a standard feature of your Arvest account. We have included a Welcome Kit that outlines how you can take advantage of the breadth of features included in this service, such as receiving alerts and requesting copies of your credit report.

2. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial one-year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. A 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). Here is a summary of your major rights under FCRA. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights. In addition, you have the right to request that each of the three consumer reporting agencies listed below send you a free copy of your credit reports once every twelve months for your review.

6. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Identity thieves may wait to use stolen personal information at different times. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. Please also call the consumer reporting agency at the phone number on the report. Please also notify us of the suspicious activity. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600

Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your bank account information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account.

For Maryland and North Carolina Residents: You may also contact and obtain information about identity theft from your state attorney general at:

- **Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202**
Main number: 410-576-6300 or Toll-free: 1-888-743-0023 (<http://www.marylandattorneygeneral.gov>)
- **North Carolina Attorney General's Office**, 9001 Mail Service Centre, Raleigh, NC 27699
Main number: 1-919-716-6000 or Toll-free: 1-877-566-7226 (www.ncdoj.gov)

For Massachusetts Residents: Under Massachusetts law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Iowa and Oregon Residents: You may also report suspected identity theft to your state's local law enforcement or your state's attorney general at:

- **Office of the Attorney General of Iowa, Consumer Protection Division**
Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106
Main number: 515-281-5926 or Toll-free: 1-888-777-4590 (consumer@ag.iowa.gov)
- **Oregon Attorney General's Office**
Main number (877) 877-9392 (<https://www.doj.state.or.us/>)