

July 29, 2023

Via Electronic Mail

Brenna Bird, Attorney General
Office of the Attorney General
Hoover State Office Building
1305 E. Walnut Street
Des Moines IA 50319

Re: Aven Financial, Inc. – Notice of Security Incident

Dear Sir or Madam:

I am writing to provide notification of an incident at Aven Financial, Inc. (“Aven”). Aven offers consumer financial products, including credit cards. Aven’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, Aven does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

Aven was recently informed by a security researcher associated with a reputable third-party security research platform that he was able to access an internal, in-development storage system containing personal information, through a temporary vulnerability in that system. Aven took immediate steps to secure that system. Below is the timeline of events:

- On July 17, 2023, a security researcher gained unauthorized access to that system, and within 45 minutes, informed Aven of this vulnerability.
- Information related to 25 Aven Home (an Aven product) users was accessed.
- Information related to 662 Aven Advisor (a second Aven product) users was accessed.
- Within 45 minutes of learning of this vulnerability, Aven eliminated the risk of future access through that vulnerability.
- Aven then immediately launched an investigation in consultation with outside counsel.
- Aven’s investigation has indicated that the only person to access the vulnerability was the security researcher.
- The security researcher began actively cooperating with Aven immediately upon discovering the vulnerability.

Based on its ongoing investigation and document review, Aven discovered, on July 17, 2023, that certain files containing personal information were accessed from the internal storage system. The type of personal information exposed varied but may have included the following of the affected residents: name, financial account information, SSN, demographics (such as address or date of birth), and e-mail address.

The investigation, including the review of server logs and the evidence cited below, indicates that no other unauthorized individual had access to the internal storage system. We have not received any reports of identity fraud or improper use of any information as a direct result of this incident. The security researcher has attested to the fact that all personal

information collected as part of his research was promptly deleted and has not been disclosed to any other individual. Despite the low risk of harm, and out of an abundance of caution, Aven wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Aven is providing the affected residents with written notification of this incident commencing on or about July 28, 2023 in the same form as the enclosed consumer notice letter. Aven is offering many of the residents, as appropriate per state law and other factors, complimentary twenty-four month memberships with a credit protection service. Aven is also advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Aven, protecting the privacy of personal information is a top priority. Aven is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it, and continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions concerning this notification, please contact Aven at RChillemi@aven.com. Thank you.

Very truly yours,

Aven Financial, Inc.

Encl.

<<Name 1>> <<Name 2>>
<<Address 1>> <<Address 2>>
<<City>><<State>><<Zip>>

Notice of Data Breach
Important Information
Please Review Carefully

<<Date>>

Dear <<Name 1>> :

Aven Financial, Inc. (“Aven”) is committed to protecting the personal information we collect and maintain. We are writing to notify you of a data security incident that may have involved some of your personal information. We apologize for any inconvenience this may cause you. While we have no evidence that any personal information was compromised, we wanted to inform you of this event out of an abundance of caution. This notice explains the incident, measures we have taken, and some steps you may consider taking in response.

Aven was recently informed by a security researcher that he was able to access an internal, in-development storage system containing personal information, through a temporary vulnerability in that system. Aven took immediate steps to secure that system. Below is the timeline of events:

- On July 17, 2023, a security researcher gained unauthorized access to that system, and within 45 minutes, informed Aven of this vulnerability
- Within 45 minutes of learning of this vulnerability, on that same day, Aven remediated and eliminated the risk of future access through that vulnerability
- We determined that the only person to access the vulnerability was the security researcher, who is actively cooperating with Aven

We have taken further steps to heighten the security of your information and our systems, including the launch of a bug bounty program to continuously identify risks as part of Aven’s security research program.

We are offering you a complimentary twenty-four month subscription to credit protection services. For more information on these services, including instructions on how to activate your complimentary subscription, please visit the website below and also see the additional information provided with this letter.

We are always committed to maintaining the privacy and security of personal information. Please see below for responses to frequently asked questions.

What Happened?

On July 17, 2023, Aven was informed by a third-party security researcher who is affiliated with a well-known security research platform that he was able to access an in-development storage system containing personal information. Aven remediated and eliminated the vulnerability within 45 minutes of learning of it. We are thankful that the security researcher disclosed this promptly.

What Information was Involved?

Information that may have been involved includes your name, SSN, date of birth, and other information. No passwords were accessed as part of this incident.

What We Are Doing.

Our immediate investigation established that the security researcher was the only person to access these files; no other unauthorized person accessed the data. Although we eliminated that risk within 45 minutes of learning of this vulnerability from the researcher, we continue to always invest in additional technical safeguards to prevent future incidents.

What You Can Do.

While no passwords were accessed as part of this incident, cybersecurity experts recommend changing passwords every 90 days. Consider placing a Fraud Alert and/or Security Freeze on your credit files, and applying multi-factor authentication on your financial accounts. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

If you have any further questions regarding this incident, please visit <https://www.aven.com/datasupport> to schedule a toll-free call on our dedicated and confidential response line through the link provided. This response line is staffed with professionals familiar with this incident, and knowledgeable on what you can do to protect your information. The response line appointments are Monday through Friday, from 9 a.m. to 3 p.m. Pacific.

Sincerely,

Aven Financial, Inc.

– OTHER IMPORTANT INFORMATION –

Enrolling in Complimentary 24-Month Credit Monitoring.

To enroll in credit protection services, please visit <https://www.avenadvisor.com/creditprotection> to register through the link provided.

Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 24-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

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 national credit reporting companies using the information below and following the stated directions, or by sending a request in writing, by mail, again 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, DOB, SSN 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 protection services as described above, you will need to remove the freeze in order to sign up for the credit protection services. After you sign up for the services, you may refreeze your credit file.

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.

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.

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, New York, 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>)
- **New York Attorney General's Office, Bureau of Internet and Technology**
Helpline: 1-800-771-7755 (<https://ag.ny.gov/internet/resource-center>)
- **NYS Department of State's Division of Consumer Protection**
Helpline: 1-800-697-1220 (<https://www.dos.ny.gov/consumerprotection>)
- **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, if applicable, 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, Oregon, and Rhode Island 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/>)
- **Rhode Island Attorney General's Office, 150 South Main Street, Providence, Rhode Island 02903**
Main number: (401) 274-4400 (<http://www.riag.ri.gov>)