

September 13, 2024

Colman D. McCarthy

VIA email to idtheft@oag.state.md.us
Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

2555 Grand Blvd.
Kansas City, Missouri 64108
t 816.474.6550
dd 816.559.2081
f 816.421.5547
cdmccarthy@shb.com

RE: Savi Solutions PBC

Dear Sir/Madam:

I am writing on behalf of Savi Solutions PBC, a technology company based in Washington, D.C., to notify you of a security incident involving the personal information for one Maryland resident.

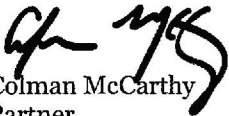
On August 26, Savi Solutions was alerted to a potential vulnerability in how it integrates and uses a third-party software application as part of its business. The vulnerability resulted in a small portion of Savi Solutions' environment being accessible from the internet. Upon learning of the vulnerability, Savi Solutions immediately located and remediated it. It is also undertaking a comprehensive review of other third-party applications it uses and how they are configured, to protect against similar vulnerabilities.

Savi Solutions also undertook an investigation to determine what, if any, data might have been impacted while the vulnerability was in place. That investigation determined that the full name, address, and Social Security number for one Maryland resident were present in the impacted software application. Savi Solutions has not been able to confirm that any personal information was actually subject to unauthorized access, nor is it aware of any unauthorized use of that information. Nevertheless, out of an abundance of caution and in the interests of transparency, it is providing notice to the potentially impacted individual.

On September 13, Savi Solutions provided notice to the Maryland resident, and we have attached a template of that notification letter for your review. Savi Solutions is providing a complimentary one-year membership to Experian IdentityWorks credit monitoring.

Please contact me if you have any questions or need any additional information regarding this incident.

Sincerely,


Colman McCarthy
Partner

Encl.





1032 15th St NW #282
Washington, DC 20005

September 13, 2024

VIA U.S. MAIL

<Name>

<Address>

<City>, <State> <ZIP>

Dear <Name>,

At Savi, we're committed to providing a better way for borrowers to deal with student debt. This includes a commitment to protect the information of our customers that we collect. Unfortunately, like many organizations, we recently experienced an incident that may have exposed some of your personal information. We took immediate action to respond to and investigate the incident, and are now reaching out to provide you information and an opportunity to enroll in free credit monitoring.

WHAT HAPPENED AND WHAT WE ARE DOING

On August 26 this year, we were alerted to a potential vulnerability in how we integrate and use a third-party software application as part of our business. The vulnerability resulted in a small portion of our environment being accessible from the internet. Upon learning of the vulnerability, we immediately located and remediated it. We are also undertaking a comprehensive review of other third-party applications we use and how they are configured, to protect against similar vulnerabilities.

WHAT INFORMATION WAS INVOLVED

Our investigation determined that your full name, address, and Social Security number were present in the impacted software application. We have not been able to confirm that your personal information was actually subject to unauthorized access, nor are we aware of any unauthorized use of that information. Nevertheless, out of an abundance of caution and in the interests of transparency, we are reaching out to you with this information.

WHAT YOU CAN DO

Attached to this letter you can find information on steps you can take to protect yourself. In addition, we are offering you a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of personal information. To register, please:

- Ensure that you **enroll by:** <date> (Your code will not work after this date.)
- **Visit the Experian IdentityWorks website to enroll:** <https://www.experianidworks.com/<code>>
- Provide your **activation code:** <code>

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by <date> and provide them engagement number <code>.

FOR MORE INFORMATION

If you have additional questions, you may contact us at (855) 728-4702 or partners+legal@bysavi.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Katie Mogul".

Katie Mogul
Chief of Staff

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – Review your account statements and free credit reports for the next twelve to twenty-four months for unauthorized financial activity.

- You should confirm that your financial institutions have the correct address on file for you and that all charges on your accounts are legitimate. If you discover errors or suspicious activity, you should immediately contact the financial institution and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit-reporting agencies. We recommend you do so and if the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a free, cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

Contact information for the three nationwide credit-reporting agencies:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, (800) 685-1111.
- Experian, PO Box 2104, Allen, TX 75013, www.experian.com, (888) 397-3742.
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, (800) 888-4213.

Federal Trade Commission

- 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 FTC. Online guidance regarding steps you can take to protect against identity theft is available from the FTC at the website listed below.
- You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call (877)-ID-THEFT ((877) 438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.