
To whom it may concern:

Array maintains certain personal information in its role as a service provider to our financial institution and fintech partners. This information is stored in a secure database, and can only be accessed by the Array partner with the consumer's direction and consent.

On or about June 15, 2023, we confirmed that the name and social security number of one Maryland resident may have been inadvertently transmitted electronically to, but not necessarily viewed or otherwise accessed by, another consumer.

This incident was not the result of malicious action by third parties, but instead occurred when an improperly scoped variable in Array's application codebase caused a race condition (two processes tried to access the same resource at the same time). The conditions necessary to cause this condition are extremely rare. Array updated the application code to prevent this issue from reoccurring. Subsequent testing and updated processes were implemented as additional safeguards.

A sample notification letter, which will be sent via US Mail on July 17, 2023, is attached.

Please let me know if you have any additional questions.

Thanks,

Andrew

Andrew Davidson

Head of Litigation

andrew.davidson@array.com

[Book a meeting](#)



[First Name] [Last Name]
[Street Address]
[City, State, and Postal Code]

Dear [First Name]:

We are sending this letter to you to inform you that Array US, Inc. ("Array") recently discovered an incident potentially involving your personal information.

Array maintains certain personal information in its role as a service provider to our financial institution and fintech partners. This information is stored in a secure database, and can only be accessed by the Array partner with the consumer's direction and consent.

On or about June 15, 2023, we confirmed that your name and social security number may have been inadvertently transmitted electronically to, but not necessarily viewed or otherwise accessed by, another consumer.

This incident was not the result of malicious action by third parties, but instead occurred when an improperly scoped variable in Array's application codebase caused a race condition (two processes tried to access the same resource at the same time). The conditions necessary to cause this condition are extremely rare. Array updated the application code to prevent this issue from reoccurring. Subsequent testing and updated processes were implemented as additional safeguards.

Although we are not aware of anyone's information being misused, as an added security measure, we will provide you with two years of complimentary identity theft protection through LifeLock or an equivalent provider of Array's choosing. The offer to receive complimentary protection will expire on October 18, 2023. To obtain your membership and get protection at no cost to you, please contact legal@array.com or call 844-582-0637.

Additionally, we remind you to remain vigilant for signs of fraud or identity theft. We encourage you to take the following steps to protect yourself from harm:

- **Monitor Your Credit Report and Accounts.** You should closely monitor your credit report, credit cards, bank accounts, and online accounts for signs of any unauthorized or suspicious activity that may indicate fraud or identity theft, and be aware that criminals may attempt to send you targeted emails seeking to obtain other confidential information from you or may otherwise try to use your personal information. If you notice any illegal, unauthorized or suspicious activity, always report it to law enforcement, and the appropriate financial institution and government authorities.
- **Request a Free Initial Fraud Alert.** You should consider placing a free initial fraud alert on your credit report. An initial fraud alert lasts for ninety (90) days, and warns any creditor who orders a credit report during that period that they must not extend new credit in your name without first verifying that you are the applicant. You can renew the initial fraud alert for additional periods of ninety (90) days. If you are a victim of identity theft, you can request an extended fraud alert. To request a fraud alert, call any one of the three national credit reporting agencies:

Equifax

(888) 766-0008
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
Equifax Consumer Fraud Division
P.O. Box 105139
Atlanta, GA 30348-7289

Experian

(888) 397-3742
www.experian.com/fraud
Experian Fraud Center
P.O. Box 2002
Allen, TX 75013

TransUnion

(800) 680-7289
www.transunion.com/fraud
TransUnion Fraud Victim
Assistance Dept.
P.O. Box 2000
Chester, PA 19016

You only need to contact one of the three national credit reporting agencies to place a fraud alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. If you do not receive a confirmation from a credit reporting agency, you should contact that agency directly to place a fraud alert.

- **Consider Asking for a Freeze on Your Credit Report.** You may also consider asking for a freeze on your credit report. Freezing your credit report prevents a credit reporting agency from providing your credit report or credit score to anyone without your permission. You should ask about a credit freeze when you place a fraud alert on your account. There are, however, some disadvantages to a credit freeze. You will need to lift the freeze whenever you want to open a new credit account or get a new loan. This will take time and may delay your credit transaction. The credit reporting agency can charge a fee for establishing and lifting a freeze. For more information about credit freezes, how to request them, and their advantages and disadvantages, go to: <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.
- **Review Federal Trade Commission's Identity Theft Information.** You should review information about personal identity theft and fraud at the Federal Trade Commission ("FTC") website (<http://www.consumer.gov/idtheft>). You may also enter your information into the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement agencies for use in their investigations, at <https://www.identitytheft.gov/> or by calling 1-877-ID-THEFT. If at some point you believe any bank or credit accounts have been used fraudulently, the FTC recommends that you close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at <https://www.identitytheft.gov/>) when you dispute new unauthorized accounts.
- **Maryland Attorney General's Office.** The Maryland Attorney General provides additional information at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/databreech.aspx>. The Consumer Protection Division Office can be contacted at 866-366-8343, or visited at 15045 Burnt Store Road, Hughesville MD 20637.

We apologize for this incident and any inconvenience and stress that this situation has caused you. We are committed to keeping your information safe, and we want to assure you that we have taken steps to prevent this type of incident in the future.

Please do not hesitate to contact us with any questions about this incident or to request additional information, at legal@array.com or by phone at 844-582-0637.

Sincerely,

Alem Sendaba
General Counsel