



6100 Merriweather Dr., Suite 600
Columbia, MD 21044
410-884-2900

November 27, 2023

BY EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

On behalf of Advarra, Inc. ("Advarra"), and pursuant to Md. Code Ann. Comm. Law § 14-3504(h), this letter provides notice of a cybersecurity incident involving Maryland residents.

On October 26, 2023, Advarra learned that an unauthorized third-party accessed a single Advarra employee's user account via sim swapping of the employee's phone number. This access did not result in any software, such as malware or ransomware, being installed in Advarra's environment; accordingly, there was no disruption to Advarra's operations. The unauthorized third-party did acquire a limited amount of company data, including data from the human resources systems relating to current and former employees.

Immediately after becoming aware of this, Advarra took steps to contain the incident, including retaining outside cybersecurity experts to support the investigation. This investigation found that the unauthorized third-party first gained access to Advarra's network on October 25, 2023. Advarra was able to contain the incident the next morning. There has been no further unauthorized access to Advarra's network since the incident was contained on October 26, 2023. Advarra also notified law enforcement on October 26, 2023.

As of November 1, 2023, Advarra provided informal notice to its employees and provided employees with 24 months of free identity theft and credit monitoring services through Kroll. Advarra is in the process of providing the same service to all former employees while evaluating any impact to non-employee data.

On November 5, 2023, the unauthorized third-party posted some Advarra human resources data to the dark web. While Advarra is determining the exact scope of affected records, a preliminary analysis shows that personal information of approximately one-hundred (100) Maryland residents was posted. The personal information acquired included first names and last names, Social Security numbers, passport numbers, physical addresses, phone numbers, and salaries. Advarra anticipates sending these individuals

formal notice on November 29, 2023 via U.S. mail. A sample notification letter is enclosed.

Since this incident, Advarra has taken measures to ensure that the unauthorized third-party no longer has access to Advarra's systems, and is continuing to monitor and improve Advarra's capabilities to detect any persistent threats. Specifically, multi-factor authentication via SMS has been disabled.

As noted above, our investigation of the incident is ongoing. We will provide your office with any material updates resulting from that investigation. Advarra takes this matter very seriously and is committed to answering any questions you may have. If you have any questions regarding this submission, please do not hesitate to contact me at marco.capasso@advarra.com or 917-270-6856.

Respectfully yours,

Marco Capasso
General Counsel
Advarra, Inc.
6100 Merriweather Dr., Suite 600, Columbia, MD 21044

Sample Individual Notification Letter



6100 Merriweather Dr., Suite 600
Columbia, MD 21044
410-884-2900

<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

<<Date>>

NOTICE OF SECURITY INCIDENT

Dear <<Name 1>>:

We are writing to let you know about a cybersecurity incident that affected some of your information. We are providing you with information about the event, our response, and additional measures you can take to help protect yourself.

What Happened?

On October 26, 2023, Advarra was made aware that an unauthorized third-party accessed a single Advarra employee's user account, and acquired a limited amount of company data. We promptly contained the incident by disabling the employee's account and immediately launched an investigation into the nature and scope of the unauthorized access into our system. Through the investigation, we learned that the unauthorized activity began on October 25, 2023. We then conducted a review of the records to confirm the identities of individuals potentially affected by this event.

What Information Was Involved?

The following types of your information were downloaded by the third party: name, social security number, passport information, employee number, employment status, street address, city, ZIP code, phone number, and salary information.

What We Are Doing.

We take this event and the security of information in our care seriously. Upon learning of this incident, we took immediate steps to disable the affected account, launch a comprehensive investigation, and assess the security of our systems. We also engaged cybersecurity experts. We confirmed containment of the incident on October 26, and since then have seen no further unauthorized access to any portion of our network.

While we are unaware of any identity theft or fraud related to information taken acquired in this incident, as an additional precaution, we have previously provided you with credit monitoring services for 24 months. You should have already received a letter with your personalized activation code and directions on how to enroll. We encourage you to take advantage of these services.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors and to report suspected identity theft incidents to the institution. Please also review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring services that we are offering.

For More Information.

Please be assured that we are taking steps to address the incident and to protect the security of your data. If you have any questions about this notice or the incident, please feel free to contact us at cybersecurity_questions@advarra.com.

Sincerely,

The Advarra Team

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Kroll's Monitoring Services

To help relieve concerns and restore confidence following this event, we have secured the services of Kroll to provide identity monitoring at no cost to you for 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.¹

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional Information

- **Credit Monitoring.** You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers

¹ 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.

wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file

a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For Massachusetts residents, you have the right to obtain any police report filed in regard to this event. 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 New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. For <<Data Owner>> and its affiliates, there are approximately [#] Rhode Island residents that may be impacted by this event.



6100 Merriweather Dr., Suite 600
Columbia, MD 21044
410-884-2900

February 14, 2024

BY EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

On behalf of Advarra, Inc. ("Advarra"), this letter provides an update on the cybersecurity incident we first notified your Office about on November 27, 2023.

Since that time, we have continued to work with outside cybersecurity experts to ensure the ongoing security of our systems and prevent further unauthorized access. We have also continued our diligent review of the affected data. Advarra has now completed its review of the affected data. Based on this review, Advarra has determined that there are approximately fifty-two (52) additional Maryland residents whose personal information was affected, in addition to the one-hundred (100) individuals we previously notified your Office about. Depending on the individual, the personal information acquired included first names and last names, Social Security numbers, driver's license numbers, dates of birth, bank account numbers, medical record numbers, health insurance information, race, ethnicity, salary information, and taxes information.

As of November 1, 2023, Advarra provided informal notice to its employees and provided employees with 24 months of free identity theft and credit monitoring services through Kroll. As of November 21, 2023, Advarra provided the same service to all former employees. Advarra began sending formal notices to affected individuals on November 29, 2023 via U.S mail. On January 9, 2024, Advarra completed its review of the affected data and confirmed the scope of impacted individuals, and we anticipate sending all remaining notices by the week of February 12, 2024.

Advarra continues to enhance its cybersecurity measures and is continuing to monitor and improve Advarra's capabilities to detect any persistent threats. Specifically, Advarra has addressed, or has made significant progress, in the following areas: account privileges, multi-factor authentication, email verification, password policies, operating system configurations, mailbox configurations, user verifications, and user device policy.

Advarra takes this matter very seriously and is committed to answering any questions you may have. If you have any questions regarding this submission, please do not hesitate to contact me at marco.capasso@advarra.com or 917-270-6856.

Respectfully yours,

Marco Capasso
General Counsel
Advarra, Inc.

6100 Merriweather Dr., Suite 600, Columbia, MD 21044