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

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF SECURITY INCIDENT

Dear <<first_name>> <<last_name>>:

Advarra, Inc ("Advarra"), a provider of clinical trial support solutions to West Virginia University ("WVU"), experienced a cybersecurity incident resulting in unauthorized access to Advarra's network. After a thorough investigation, on February 21, 2024, Advarra notified WVU that the files downloaded by the third-party contained some WVU information. It was later determined that this information was related to clinical trial participants. On behalf of WVU, we are writing to inform you that this cybersecurity incident affected some of your personal information. The safety and security of personal data is very important to us, and we deeply regret that this incident occurred. This incident did not involve any access to WVU's systems, network, or electronic health records.

We place a high value on maintaining the privacy and security of the information we maintain for our customers. Importantly, we have no evidence that your information has been subject to fraud as a result of this incident. This letter explains the incident, the measures we have taken in response, and the steps you can take.

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. Advarra 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 its system. Through the investigation, Advarra learned that the unauthorized activity began on October 25, 2023. Advarra then conducted a review of the records involved to confirm the identities of individuals potentially affected by this event. With the assistance of external cybersecurity experts, Advarra has since taken a number of steps to enhance its information security. After gathering all relevant information, we told WVU about this incident on February 21, 2024. On March 19, 2024, WVU confirmed, unfortunately, some of your personal information was affected by the unauthorized third-party access.

What Information Was Involved? The personal information involved included your: <<b2b_text_1 (name and data elements)>>. It did not involve or include your medical record.

What Are We Doing? While Advarra is unaware of any identity theft or fraud related to information acquired in this incident, as an additional precaution, Advarra is providing complimentary identity monitoring services from Kroll for 24 months. The identity monitoring services available include Credit Monitoring, Fraud Consultation and Identity Theft Restoration services, and instructions for activating these services are included in this letter.

Visit https://enroll.krollmonitoring.com to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

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

What Can You Do? Although there is no evidence that your information has been subject to fraud, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your accounts statements, and to monitor your free credit reports for suspicious activity and to detect errors. Enclosed with this letter are some steps you can take to protect your information.

For More Information. Your privacy is of utmost importance to us, and we deeply regret that you were impacted by this cybersecurity incident and any concern it may cause you. If you have any questions regarding this incident or the services available to you, additional assistance is available by calling our toll-free assistance line at (866) 983-9303, Monday through Friday from 9:00 am to 6:30 pm Eastern Time (excluding U.S. holidays).

Sincerely,

Advarra, Inc.

Steps You Can Take To Help Protect Personal Information

Activate 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 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.

[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.

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/.