[Acrisure, LLC Letterhead] or [DBA Letterhead]

<Date>

VIA U.S. MAIL

<Name>
<Company>
<Address>
<City>, <State> <ZIP>

Re: Notice of Data Breach

Dear <Name>,

We are writing to inform you of a data security breach that may have exposed some of your personal information to unauthorized persons. Although we have no evidence to suggest that any of your personal information has, in fact, been misused, we are reaching out to provide additional information and an opportunity to enroll in free credit monitoring and identify theft protection services.

WHAT HAPPENED?

On December 28, 2022, we became aware of some unusual activity on our systems. We immediately began working with cybersecurity experts to investigate and subsequently determined that an unauthorized third party gained access to a portion of our computer network that contained a number of files, including those with personal information. Based on our investigation, we believe the unauthorized access occurred from December 1, 2022 to January 28, 2023. Once we identified the data that may have been affected, we promptly engaged a data-review firm to determine what information was contained in those files. We received the results of that review in late August. We have been working since then to identify the affected individuals and the correct addresses for them.

WHAT INFORMATION WAS INVOLVED?

Our investigation determined that some combination of the following types of personal information related to you may have been impacted: [data elements].

WHAT WE ARE DOING?

We hired third-party experts to help address the situation, investigate the unauthorized activity, and further secure our systems to protect the personal information and other data stored on them. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO?

We encourage you to remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring free credit reports. Enclosed with this letter you will find additional steps you can take to help protect yourself.

In addition, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for [one year or two years]. 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, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

- Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.
- You have until <<Date>> to activate your identity monitoring services.
- Membership Number: <<Member ID>>

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

Additional information describing your services is included with this letter.

FOR MORE INFORMATION:

We take the privacy and security of the information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you. Should you have any questions, you can contact us at _____, and one of our representatives will be happy to assist you.

Thank you for your understanding and patience.

Sincerely,

Jorel Van Os, CISM, CEH
Chief Information Security Officer

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – Review your account statements and free credit reports.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company 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. 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 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. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.
- 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.

Report suspicious activity – If you believe you are the victim of identity theft, consider notifying your Attorney General, local law enforcement, or the Federal Trade Commission. You can also file a police report concerning the suspicious activity and request a copy of that report.

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. For any services not described above, please be aware that the consumer reporting agencies may charge you a fee.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW Washington, DC 20580 (202) 326-2222 www.ftc.gov	P.O. Box 740241 Atlanta, GA 30374 (800) 685-1111 www.equifax.com	P.O. Box 2104 Allen, TX 75013 (888) 397-3742 www.experian.com	P.O. Box 2000 Chester, PA 19016 (800) 888-4213 www.transunion.com

For Maryland Residents: 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.

For North Carolina Residents: the North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; (800) 771-7755; www.ag.ny.gov.

For Washington, D.C. Residents: the District of Columbia Attorney General may be contacted at: Office of the Attorney General, 400 6th Street, NW, Washington, D.C. 20001; (202) 727-3400; https://oag.dc.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 (401) 274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are three Rhode Island residents impacted by this incident.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau 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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.

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.