March 14, 2024

Maryland Attorney General Office
Director of Consumer Affairs & Business Regulation
idtheft@oag.state.md.us

Dear Attorney General Brown,

Pursuant to Md. Code Com. §14-3501 et seq., we are writing to notify you of a breach of security involving **two** (2) Maryland state residents.
`

1. **Brief Description**
   By way of background, Bonney Forge/WFI ("Bonney Forge") is a forge for steel fittings and valves headquartered in Mount Union, PA. Bonney Forge operates exclusively on a business-to-business basis. Personal data Bonney Forge processes are limited to employee or contractor information.

   Bonney Forge discovered suspicious network activity resulting in a partial systems outage on January 26, 2024. Bonney Forge immediately launched its incident response procedures, engaged external experts to identify the cause of the incident; and notified the FBI.

   Bonney Forge identified that the incident was a ransomware attack deployed by the Threat Actor (TA), Cactus. Over the days following the initial discovery, Bonney Forge took steps to contain, remediate, and quickly restore systems securely. Containment and remediation were accomplished within 3 days' time.

   Bonney Forge, with the assistance of external third-party experts and breach legal counsel conducted a thorough investigation into the incident determining the breach period began on January 22, 2023. While Bonney Forge pre-breach preparedness ensured high fidelity back-ups were available and systems were securely restored, the company also undertook a data mining exercise to identify files and potentially impacted individuals. It is at this stage following the output of the data mining exercise that Bonney Forge has become aware of the involvement of some personal data relating to **two** (2) individuals that may be Maryland residents. It is on that basis that Bonney Forge is notifying the Maryland Attorney General's office and potentially affected individuals.

2. **Notice to Individuals.**
   Notice of the security incident is expected to be sent the week of March 10, 2024. Bonney Forge is offering Experian credit and identity monitoring services for 24 months to the two potentially affected Marylanders.

3. **Sensitive Personal Information**
   The data involved in the event may have included: full name; date of birth, and social security number.

4. **Measure to Address the Security Incident**
   Bonney Forge with the assistance of external experts made focused updates to its security program before, during, and after a critical review of the Incident to further enhance its security posture around an ever-changing threat landscape, which included:

   Technical updates to the security infrastructure spanned:

   - Deployment of early detection and response agents on all endpoints;

- Increasing authentication thresholds to log into the Virtual Privacy Network (VPN);
- Blocking USB ports;
- Deploying MS Intune for enhanced security compliance on all mobile devices and applications;
- Expanded use of MFAs for access to any data applications.

Bonney Forge also made several administrative and procedural enhancements to its security program, including:

- Global password reset was executed for all domain/VPN users;
- Limits placed on VPN admin accounts and all VPN traffic is logged;
- Stale laptops not connected BF domain within 90 days are frozen until unlocked by IT;
- Local Admin accounts RBAC re-assessed by IT;
- Enhanced employee security and privacy training including phishing email testing.

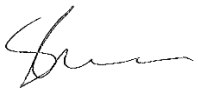
5. Bonney Forge Security and Privacy Prior to the Incident

Prior to the incident, Bonney Forge had a variety of preventative measures in place, including but not limited to administrative, technical, and physical controls consistent with ISO27001 standards. Measures included: strict password policy, Firewall protection, MFA for Microsoft applications, and access-controlled server rooms. Additionally, security and privacy policies and controls undergo a monthly review.

In addition to the above measures, since the Incident, Bonney Forge has been working to further reinforce its systems and has taken steps as described in section **4** above.

Should you require additional information, I can be reached at sleone@bonney forge.com or by phone at (713) 695-3633 EXT. 3285.

Respectfully Submitted,



Sue Leone
Executive Vice President
Bonney Forge - WFI Operations

Attachment (1)

Attachment 1 - Sample Consumer Notice & ID Protection Letter

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 14, 2024

K9580-L02-0000002 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L02 COMBINED BF MEDICAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Notice of Data Breach of Healthcare Data

Dear Sample A. Sample,

Bonney Forge/WFI is writing to make you aware of an incident that may have involved some of your personal information. We take the protection of your information seriously. We are writing to provide you with information about the incident; the steps that have been taken in response to it; and the resources available to you to help better protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened?

On January 26, 2024, a systems outage caused by ransomware was discovered in the Bonney Forge/WFI IT environment. We immediately began an investigation into the incident with help from leading external forensics experts. We quickly notified law enforcement of the event. The investigation determined that an unauthorized actor accessed the Bonney Forge network and removed certain files from it between January 22 and January 26, 2024. As a result, Bonney Forge undertook a comprehensive process to identify what information was potentially contained within the relevant files and to whom that information belonged. We are now notifying individuals whose information was potentially impacted by the incident.

What Information Was Involved?

Our review determined Protected Health Information in health insurance records related to adult individuals may have been subject to unauthorized access including: First and Last name, Date of Birth, and Social Security Number.

Upon review, we also determined health insurance records containing health information related to a minor(s) may have been subject to unauthorized access. Health information related to your minor(s) that may have been involved includes: First and Last name, Date of Birth, and Social Security Number.

What We Are Doing

The threat has been removed. Our systems have been secured and we have taken steps to prevent this type of threat in the future. To help relieve concerns and restore confidence following this incident, we have secured the services of Experian IdentityWorks℠ to provide identity monitoring at no cost to you. Experian IdentityWorks℠ provides you with superior identity detection and resolution of identity theft.

Activation Code:

- Sample A. Sample – Provide your activation code ABCDEFGHI

0000002

BONNEY FORGE

To activate your membership and start monitoring your personal information please follow the steps below.

- Ensure that you **enroll by**: **June 30, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Engagement number **B117508**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you have questions about the product, need assistance with identity restoration for yourself or your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **833-918-7223** by **June 30, 2024.** Be prepared to provide engagement number listed above as proof of eligibility for the identity restoration services by Experian.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **833-918-7223**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

BONNEY FORGE

What You Can Do.

Please review the enclosed "**Additional Resources**" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information.

If you have questions, please email eventinfo@bonneyforge.com.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Sue Leone
Executive Vice President-WFI Operations

0000002

BONNEY FORGE

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. 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.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well):

(1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

BONNEY FORGE

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.