

Ty E. Dedmon
One Federal Place
1819 5th Avenue N
Birmingham, AL 35203
tdedmon@bradley.com
205.521.8729 direct
205.488.6729 fax



July 12, 2023

CONFIDENTIAL
VIA OVERNIGHT MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202



Re: Notice of Data Breach

To the Office of the Maryland Attorney General:

I'm writing to notify your office of a data incident on behalf of our client, Brett/Robinson Gulf Corporation (hereinafter "Brett/Robinson"). Brett/Robinson is located at 3259 Gulf Shores Parkway, Gulf Shores, AL 36542. The investigation is ongoing, and this notice is based on information known as of the date of this letter.

Nature and Scope of Breach

On April 27, 2023, Brett/Robinson experienced a business-wide ransomware incident as a result of an unauthorized third party¹ gaining access to its system, which prompted Brett/Robinson to immediately respond and begin an investigation. As part of that investigation, a global forensic cybersecurity expert was retained. Based on the investigation, the breach of Brett/Robinson's network started in or around April 22, 2023. The investigation uncovered that, between April 22 and May 1, 2023, the threat actor performed network reconnaissance, performed remote administration tasks, and deployed mechanisms to bypass Brett/Robinson's cybersecurity safeguards to further access its system; including deploying a program that can be used to exfiltrate data from the victim's network. On May 16, 2023, the investigation confirmed that information may have been acquired by the threat actor on April 25, 2023.

Brett/Robinson promptly began a review of potentially affected files to determine what information may have been involved in this incident. Brett/Robinson continues to investigate this incident. Brett/Robinson notified the Federal Bureau of Investigation but did not delay any individual notification for any law enforcement investigation.

¹ The threat actor identified themselves as "Abyss Locker."

Breach Investigation and Remediation

The investigation is still in progress, but Brett/Robinson believes the incident has been contained. Brett/Robinson continues to monitor its systems for any suspicious activity. Brett/Robinson has also implemented additional security features, such as endpoint protection and monitoring, a forced global reset of all passwords, and forced multi-factor authentication (MFA). Brett/Robinson continues to evaluate ways to further enhance the security of its systems.

Impacted Information

Based on Brett/Robinson's investigation to date, the personal information potentially accessed or acquired may have included name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, social security number and/or financial account information, username and password, and other information such as phone number, address, and email address.

Notice to and Number of State Residents

Brett/Robinson has not yet confirmed the extent to which personal information was exposed as a result of this incident. However, to avoid delay, Brett/Robinson notified all potentially affected individuals via written mail notice on June 16, 2023, which includes 6 currently known Maryland residents.

Brett/Robinson has arranged to provide twenty-four (24) months of free credit monitoring and identity protection services through Experian IdentityWorksSM to the individuals whose information may have been involved. Brett/Robinson has established a call center, through Experian, to answer questions and provide support to affected individuals.

Additionally, Brett/Robinson is providing impacted individuals with guidance on how to protect against identity theft and fraud. Brett/Robinson is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. A sample copy of the written notification to Maryland residents is enclosed hereto.

If you require any additional information on this matter, please do not hesitate to contact me.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Ty E. Dedmon', with a stylized, cursive script.

Ty E. Dedmon

Enclosure (Sample Individual Notice)



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

June 16, 2023

J5903-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



NOTICE OF DATA BREACH

Dear Sample A. Sample:

Brett/Robinson Gulf Corporation, (hereinafter "Brett/Robinson"), is writing to inform you of a data security incident that may have involved your personal information. Brett/Robinson takes the privacy and security of your personal information very seriously. This letter provides information about the incident and resources available to help you protect your information.

What Happened? On April 27, 2023, we experienced a business-wide security incident that resulted in an unauthorized third party gaining access to our system. In response, we promptly took steps to investigate the incident. As part of that investigation, a global forensic cybersecurity expert was retained. Based on the investigation to date, it appears the breach of our network started in or around April 22, 2023. On May 16, 2023, the investigation confirmed that information may have been acquired by the unauthorized third party. We promptly began a review of potentially affected files to determine what information may have been involved in this incident. We notified the FBI but have not delayed this notification for any law enforcement investigation.

What Information Was Involved? The personal information involved may have included your name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, social security number and/or financial account information, username and password, and other information such as phone number, address, and email address.

What We Are Doing. Our investigation is still in progress, but Brett/Robinson, with the help of our forensic expert, believes the incident has been contained. We continue to monitor our systems for any suspicious activity. We have implemented additional security features, such as additional endpoint protection and monitoring, as well as resetting all employee passwords. We continue to evaluate ways to further enhance the security of our systems.

To help protect your identity, we are offering you complimentary credit monitoring and identity protection services through Experian IdentityWorksSM a period of 24 months. Please see the enclosed Reference Guide for enrollment details and instructions on how to enroll.

What You Can Do. In addition to enrolling in complimentary credit monitoring and identity protection services, the Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to remain vigilant against potential identity theft and fraud by carefully reviewing credit reports and account statements to ensure that all activity is valid.



For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 855-797-1895 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B097433.

Sincerely

Bill Brett - President

Brett Robinson Gulf Corp.

Reference Guide

Enroll in Free Credit Monitoring and Identity Protection Services:

To help protect your identity, we are offering free access to Experian IdentityWorksSM for 24 months.

This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by September 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 855-797-1895 by **September 30, 2023**. Be prepared to provide engagement number **B097433** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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 specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARETM: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- \$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.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: Carefully review account statements and credit reports to ensure that all of your account activity is valid. Report any questionable charges promptly to the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Order Your Free Credit Report: To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form (available at www.annualcreditreport.com) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You also can contact one or more of the following three national consumer reporting agencies:

- **Equifax:** P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, <https://www.equifax.com/personal/credit-report-services>
- **Experian:** P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com/help
- **TransUnion:** P.O. Box 2000, Chester, PA 19016, 1-800-916-8800, www.transunion.com/credit-help

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report.

Consider Placing a Fraud Alert on Your Credit Report: You have the right to place an initial or extended "fraud alert" on your credit report at no cost. An initial fraud alert lasts 1-year and can be renewed as many times as desired. 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which



is a fraud alert lasting seven years. To place a fraud alert on your credit report, contact any one of the consumer reporting agencies listed below. The agency you contact will then contact the other two credit agencies.

- **Equifax Information Services:** P.O. Box 105069 Atlanta, GA 30348-5069, 1-800-525-6285, or by visiting: <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
- **Experian Fraud Alert:** P.O. Box 9554, Allen, TX 75013-9554, 1-888-397-3742, or by visiting: <https://www.experian.com/fraud/center.html>
- **Transunion:** P.O. Box 2000 Chester, PA 19016-2000, 1-800-916-8800, or by visiting: <https://www.transunion.com/fraud-alerts>

Request a Security Freeze: You have the right to put a security freeze on your credit file at no cost. A security freeze will ensure potential creditors and other third parties are unable to access your credit report without your consent to lift the freeze. As a result, a security freeze may interfere with or delay approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Unlike a fraud alert, you must separately place a security freeze on your credit file with each consumer reporting agency. Pursuant to federal law, you cannot be charged to place or lift a security freeze.

In order to request a security freeze, you will need to provide some or all of the following information to the consumer reporting agency, depending on whether you do so online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Should you wish to place a security freeze, please contact the three major consumer reporting agencies listed below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
<https://www.experian.com/freeze/center.html>

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-916-8800
<https://www.transunion.com/credit-freeze>

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

Additional Information: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft at: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338) and TTY: 1-866-653-4261, www.identitytheft.gov/. The FTC also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud.

Brett/Robinson Gulf Corporation: Brett/Robinson Gulf Corporation, located at 3259 Gulf Shores Parkway, Gulf Shores, AL 36542 (mailing: P.O. Box 4009, Gulf Shores, AL 36547) can be reached at: (800) 221-6180.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia Residents: You may contact the D.C. Attorney General's Office to obtain information about steps to take to avoid identity theft: D.C. Attorney General's Office, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, (202) 442-9828, www.oag.dc.gov.

Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, (410) 528-8662 or (410) 576-6491, or visit <http://www.marylandattorneygeneral.gov/>.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: New York Attorney General Consumer Frauds & Protection Bureau, (800) 771-7755, <https://www.ag.ny.gov> and or New York Department of State's Division of Consumer Protection, (800) 697-1220, <https://www.dos.ny.gov>.

North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: North Carolina Department of Justice, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6000, www.ncdoj.gov.

Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

Rhode Island Residents: You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General Consumer Protection Division, 150 South Main Street, Providence, RI, 02903, (401) 274-4400, www.riag.ri.gov. There are approximately 52 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

<https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores/>

You also have certain rights under the Fair Credit Reporting Act (FCRA): You have rights pursuant to the FCRA, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your 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.



NOTICE: This correspondence is sent only for informational purposes and/or for the purpose of compliance with the loan documents and/or applicable law. You may be afforded certain protections under the United States Bankruptcy Code. By this correspondence, we are not attempting to collect a debt, impose personal liability, or in any way violate the provisions of the United States Bankruptcy Code. For any questions related to the bankruptcy, please contact your bankruptcy attorney.