MARNELL COMPANIES
CONSULTING • ARCHITECTURE • DESIGN • BUILD
MANAGEMENT • PROPERTIES • TRANSPORTATION

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

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

NOTICE OF <<B2B_TEXT_1(SUBJECTLINE)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Marnell Companies recently discovered an incident that may affect the security of some of your information. We take this incident seriously, and write to provide you with information about the incident, our response, and steps you can take to protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened?

On March 23, 2021, Marnell discovered suspicious activity within its network which it promptly investigated. The investigation revealed an unauthorized actor had gained access to a portion of the network, removing certain files before encrypting network files. Marnell conducted an investigation and determined that the network was impacted by a CLoP variant of ransomware, which prevented access to certain files on the system. We immediately reviewed the locations subject to unauthorized access to confirm what information was present on these locations. We completed this review around March 29, 2021, at which time we confirmed the individuals whose information was present. We then worked diligently to reconcile this information with our internal records in furtherance of identifying the appropriate contact information for those individuals, which we completed on April 16, 2021. We thereafter worked to provide notification to potentially impacted individuals as quickly as possible. Marnell is notifying you because your information may have been in the files removed from our network during the period of unauthorized access.

What Information Was Involved?

Our investigation determined that impacted information may include your <<b2b_text_2(DataElements)>>. There has been no evidence your data has been taken by an unauthorized actor; however, we are providing this notice as a courtesy and in an abundance of caution.

What We Are Doing.

We take this incident and the security of personal information in our care very seriously. Upon discovering this activity on our network, we moved quickly to respond to and to contain this incident. We additionally have conducted a comprehensive investigation of this activity to confirm its nature and scope. Further, we have security measures in place to protect the data on our systems and we continue to assess and update security measures and training to our employees to safeguard the privacy and security of information in our care. Further, we notified law enforcement of this event, and have been cooperating with their investigation and are also notifying regulatory authorities, as required by law.

As an added precaution we are offering you access to 12 months of credit monitoring and identity monitoring services through Kroll at no cost to you. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Your Information*. We encourage you to activate these services as we are unable to act on your behalf to do so.

What You Can Do.

We encourage you to remain vigilant against theft and fraud, to monitor your accounts for any unusual activity, and to report any instances of theft or fraud to law enforcement. You can also activate the complimentary identity monitoring services that we are offering to you. Please also review the enclosed "*Steps You Can Take to Help Protect Your Information*."

For More Information.

We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our dedicated call center at 1-???-???-????, which is available from 6:00 AM to 3:30 PM Pacific Time Monday through Friday (excluding major U.S. holidays). You can also write to Marnell at 222 Via Marnell Way, Las Vegas, NV 89119.

We sincerely regret any inconvenience or concern this incident causes you.

Sincerely,

Marnell Companies

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring

We have secured the services of Kroll to provide essential identity monitoring at no cost to you for one year. 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>>**

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 will 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.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 1-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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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
888-298-0045	1-888-397-3742	833-395-6938
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. 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. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226 or 1-919-716-6400; and online at 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 12224-0341; 1-800-771-7755; or https://ag.ny.gov.