A.B. Closing, Inc. D/B/A Kavaliro
April 24, 2020

NOTICE OF DATA BREACH

A.B. Closing, Inc. D/B/A Kavaliro ("Kavaliro") recently learned of a data security incident that involved the compromise of certain Kavaliro business email and file sharing systems. We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. This notification has not been delayed as a result of a law enforcement investigation, and we sincerely regret any concern this notification may cause you.

What Happened:

In March 2020, Kavaliro became aware of unauthorized persons who were using an imposter domain name to conduct email phishing directed at Kavaliro's customers. Kavaliro has since had the imposter domain taken down, and while investigating the imposter domain, on March 26, 2020, became aware of unauthorized access to several Kavaliro email accounts by those involved with the imposter domain. On April 11, 2020, Kavaliro was able to determine that there was also unauthorized access to multiple additional Kavaliro email accounts, as well as certain internal file management systems.

Kavaliro is unable to determine the specific time and date that the unauthorized access began or the exact number of affected individuals, but Kavaliro believes the unauthorized access began with two accounts in September 2019 and expanded to multiple accounts in March 2020. The unauthorized access continued through March 29, 2020.

What Information Was Involved:

The email accounts and file sharing systems at issue may have contained personally identifiable information present in the email accounts or internal file management systems at Kavaliro, including but not limited to names, dates of birth, phone numbers, email addresses, usernames, passwords, financial account information, and certain demographic information.

What We Are Doing:

Kavaliro takes privacy very seriously and deeply regrets this incident. After Kavaliro learned of this incident, it initiated a comprehensive IT security investigation and hired an independent forensic cybersecurity investigation firm to assist in its investigation and response. Kavaliro also notified the Federal Bureau of Investigation (FBI) and will continue to cooperate with any law enforcement investigation.

Kavaliro enabled multi factor authentication on its business systems, blocked certain foreign IP addresses, conducted global password resets, and is working continually to harden its information security infrastructure and technological practices to better prevent any future unauthorized access to its information systems.

As a precaution, and to reduce the risk that any client information could be misused, Kavaliro is offering potentially impacted individuals one year of identity monitoring services at no cost through Kroll, to include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. 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. The offer is available to potentially affected individuals whose information may have been in Kavaliro's compromised accounts at any time between September 1, 2019 and March 31, 2020. Qualifying individuals can learn more or request membership information by calling the call center at 844 978 2448. Once a membership number is received you will receive activation instructions by mail and have until July 23, 2020 to activate your identity monitoring services.

Additional information describing Kroll's services is included below in the Additional Resources section.

What You Can Do:

For tips on how to help protect yourself, please review the "Additional Resources" reference guide included below. This section includes steps you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection, monitoring account statements and free credit reports, and details on placing a fraud alert or a security freeze on your credit file.

For More Information:

For more information about this incident, or if you have additional questions or concerns, you may contact our dedicated call center directly at 844 978 2448 between the hours of 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major US holidays. Again, we sincerely regret any concern this incident may cause you.

Additional Resources

Review Accounts and Credit Reports: You can also regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll free 1 877 322 8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348 5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about preventing identity theft: Federal Trade Commission, Bureau of Consumer Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1 877 IDTHEFT (438 4338), www.ftc.gov/idtheft. North Carolina residents may also contact the North Carolina Attorney General's Office: 9001 Mail Service Center, Raleigh, North Carolina 27699; 1 877 5 NO SCAM; https://www.ncdoj.gov/protecting consumers/.

Fraud Alerts: There are also two types of fraud alerts that 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with 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 at the addresses or toll free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent and shall be provided free of charge. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since laws may differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)
General Contact:
800 685 1111
Fraud Alerts:
P.O. Box 105069, Atlanta, GA 30348
888 525 6285
Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348
888 298 0045

Experian (www.experian.com)
General Contact:
P.O. Box 2002
Allen, TX 75013
888 397 3742
Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact:
833 395 6938
Fraud Alerts
P.O. Box 2000, Chester, PA 19016
800 680 7289
Security Freezes:
P.O. Box 160, Woodlyn, PA 19094
888 909 8872

Take Advantage of Your Identity Monitoring Services

Kavaliro is providing access to the following services[1] 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 can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[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.