WHITE & CASE

February 22, 2020

VIA OVERNIGHT MAIL

New Hampshire Department of Justice
33 Capitol Street
Concord, New Hampshire 03301

White & Case PC
701 Thirteenth Street, NW
Washington, DC 20005-3807
T +1 202 626 3600

whitecase.com

Incident Notification

Dear Sir/Madam:

Our client, Jacuzzi In. ("Jacuzzi"), understands the importance of protecting the personal information it holds concerning New Hampshire residents.

Jacuzzi recently experienced a ransomware attack on its network. Jacuzzi discovered that a malicious actor had gained access to some of its systems. It immediately initiated an investigation and engaged a third party cyber security firm to assist in determining the nature and scope of the attack. The investigation determined that on December 15, 2021, an unauthorized person deployed malware to certain devices on the Jacuzzi network that encrypted data on those devices and prepared a limited number of files for removal from the network. On December 18, Jacuzzi disabled internet access to the entire environment to contain the attack. On January 27, 2021, Jacuzzi determined that certain files that were prepared for removal from the network may have contained personal information concerning current and former employees and their beneficiaries. The impacted data files contained documents that may have contained the first name, last name, Social Security number, bank account information, date of birth, and potentially health information concerning New Hampshire residents.

Jacuzzi anticipates it will provide written notice on February 23 via postal mail to two New Hampshire residents in accordance with N.H. Rev. Stat. § 359-C:20 in substantially the same form as the document enclosed herewith. The attached letter provides additional information about the data that was improperly accessed and the steps Jacuzzi has taken to remediate any vulnerabilities discovered during its investigation. In addition to notifying all three national credit reporting agencies, Jacuzzi is offering two years of free credit monitoring through Kroll to all persons whose data has been potentially accessed as a result of the breach. In addition, Jacuzzi has created a call center that potentially affected individuals can call with questions regarding the incident.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

J. Paul Pittman

T +1 202 729 2395
E paul.pittman@whitecase.com

Enclosure

February 23, 2021

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Jacuzzi values the relationship we have with our employees and understands the importance of protecting personal information. We are writing to inform you about an incident that may involve personal information relating to your employment or your status as a beneficiary of a current or former employee with Jacuzzi or BathWraps.

What Happened

Jacuzzi recently experienced a ransomware attack on its network. Jacuzzi immediately initiated an investigation and engaged a third party cyber security firm to assist in determining the nature and scope of the attack. The investigation determined that on December 15, 2021, an unauthorized person deployed malware to certain devices on the Jacuzzi network that encrypted data on those devices and prepared a limited number of files for removal from the network. On January 27, 2021, Jacuzzi determined that certain files that were prepared for removal from the network may have contained personal information concerning current and former employees and their beneficiaries. We are notifying you because some personal information concerning you or any beneficiaries you enrolled in company benefit programs may have been contained in files stored on the compromised computers.

What Information Was Involved

The impacted data files contained documents that may have contained your first name, last name, Social Security number, bank account information, date of birth, and potentially health information.

What You Can Do

While we have no indication that your personal information has been misused, we encourage you to remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your free credit reports. If you detect any unauthorized activity, you should promptly notify the appropriate institution. Please find more information on protecting your identity in the guidance attached to this letter.

What We Are Doing

We have resolved the issue and have taken steps to mitigate any potential impact. We continue to work with the third party cyber security firm to supplement and strengthen our existing security measures. We have also provided information to law enforcement about the incident. 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 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 two years of Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

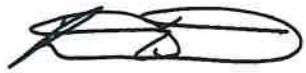
*You have until **May 25, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

For More Information

We take the safety and security of your personal information seriously. We regret any concern this may have caused you. If you have questions or need additional information, please call 1-???-???-???? between the hours of 9:00 AM and 6:30 PM Eastern Time.

Sincerely,



Brian Pierson
Chief Operating Officer

GUIDANCE FOR PROTECTING YOUR IDENTITY AND PERSONAL INFORMATION

If you are a resident of Maryland, you may contact your state attorney general about identify theft and protecting your personal information at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 or 1-410-576-6300

If you are a resident of New Mexico, you have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published the following list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf):

1. You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
2. Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
3. You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
4. You have the right to ask for a credit score.
5. You have the right to dispute incomplete or inaccurate information.
6. Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
7. Consumer reporting agencies may not report outdated negative information.
8. Access to your file is limited. You must give your consent for reports to be provided to employers.
9. You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
10. You may seek damages from violators.
11. Identity theft victims and active duty military personnel have additional rights.

If you are a resident of New York you can contact the following agencies for more information on identity theft:

New York Department of State Division of Consumer Protection, Consumer Assistance Unit 99, 1-800-697-1220, Washington Avenue, Albany, NY 12231, www.dos.ny.gov/consumerprotection

New York Attorney General, The Capitol, Albany, NY 12224, 1-800-771-7755, www.ag.ny.gov

If you are a resident of North Carolina you have the right to request a security freeze on your credit report as described below. For more information about identity theft and protecting your personal information you may contact your attorney general at:

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or 1-877-566-7226

If you are a resident of Oregon you are encouraged to report suspected identity theft to the Attorney General.

Oregon Attorney General's Office, 1162 Court Street Northeast, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us

If you are a resident of Rhode Island you have the right to file and obtain a copy of a police report, and to request a security freeze on your credit report as described below. For more information about identity theft and protecting your personal information you may contact your state attorney general at:

Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

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 request that an initial fraud alert be placed on your credit report if you are concerned about becoming a victim of fraud or identity theft. An initial fraud alert stays on your credit report one year. You may also request that an extended alert be placed on your credit report if you have already been a victim of fraud or 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.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a personal identification number ("PIN") that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security 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 security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com

TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name, address, Social Security number, and date of birth;
2. Addresses where you lived over the previous five years;
3. Proof of current address such as a utility or phone bill;
4. A photocopy of a government issued identification card;
5. If you are an identity theft victim, include a copy of the police report, investigative report, or complaint.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique PIN or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include 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 one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Finally, as a reminder you should remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. Below is contact information for the three nationwide consumer reporting agencies from which you can obtain a credit report:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

You can contact the Federal Trade Commission and/or the Attorney General's office in your state, for information about steps you can take to avoid identity theft as well as information about fraud alerts and security freezes at:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

State Attorneys General, www.naag.org/naag/attorneys-general/whos-my-ag.php

You should contact the FTC, consumer reporting agencies, local law enforcement and/or your state attorneys general immediately if you believe you are the victim of identity theft or have reason to believe your personal information has been misused. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

Kroll | A Division of DUFF&PHELPS

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.

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.