NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
1225 Seventeenth Street, Suite 3050
Denver, Colorado 80202
United States

Direct line +1 303 801 2738
erin.locker@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

October 31, 2017

By Certified Mail
Return Receipt Requested

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Rain Bird Corporation ("Rain Bird"), to inform you of a potential security incident involving the personal information of certain Rain Bird customers, including 5 New Hampshire residents. Rain Bird is notifying these individuals and outlining some steps they may take to help protect themselves.

Rain Bird was recently alerted that some of its customers were experiencing technical issues when completing an online purchase through one of Rain Bird's online stores. Rain Bird promptly began investigating this incident and engaged a third-party computer forensic firm to assist with determining what may have happened. Based upon the forensic firm's investigation, Rain Bird believes that an unauthorized individual was able to gain access to portions of the Rain Bird website and install malicious software on certain pages that was designed to capture payment card information. This incident affected purchases made between August 25, 2017 and September 15, 2017 on the following Rain Bird websites: store.rainbird.com, servicesstore.rainbird.com, and golfstore.rainbird.com. Certain information belonging to individuals who made purchases or attempted to make purchases during that time may have been affected, including name, address, email address, telephone number, order information, payment card account number, expiration date and card verification number.

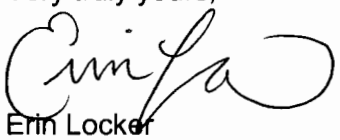
Rain Bird takes the privacy of personal information seriously, and deeply regrets that this incident occurred. Rain Bird took steps to address this incident promptly after being alerted to it,

including engaging an outside forensic investigation firm to assist with investigating the incident and remediating the situation by removing the malware and enhancing security. Upon learning that malicious software may have been affecting Rain Bird's websites on September 15, 2017, Rain Bird also took all store websites offline to ensure that no further payments would be processed through those pages. While Rain Bird is continuing to review and enhance security measures, the incident has now been contained. In addition, Rain Bird reported the incident to federal law enforcement and will cooperate with their investigation.

Affected individuals are being notified via written letter, which includes an offer for one year of complimentary identity monitoring services associated with protecting payment card data. These notifications will begin mailing on or around November 1, 2017. A form copy of the notice being sent to the affected New Hampshire residents is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2738 or erin.locker@nortonrosefulbright.com.

Very truly yours,



Erin Locker

ELL
Enclosure

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

Notice of Data Breach

Rain Bird Corporation recently became aware of a potential security incident possibly affecting the personal information of certain individuals who made a payment card purchase on one or more of the following Rain Bird store websites: store.rainbird.com, servicesstore.rainbird.com, and golfstore.rainbird.com. 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. We sincerely regret any concern this may cause you.

What Happened

We were recently alerted that certain Rain Bird customers were experiencing technical issues when completing an online purchase on the Rain Bird store website. We promptly began investigating this incident and engaged a third-party computer forensic firm to assist with determining what may have happened. Based upon the forensic firm's investigation, it appears that an unauthorized individual was able to gain access to portions of our store website between August 25, 2017 and September 15, 2017 and install malicious software on certain pages that was designed to capture payment card information.

What Information Was Involved

We believe that the incident could have affected certain information (including name, address, email address, telephone number, order information, payment card account number, expiration date and card verification number) of individuals who made a purchase or attempted to make a purchase on a Rain Bird store website between August 25, 2017 and September 15, 2017. According to our records, you made or attempted to make a payment card transaction during this period so it's possible that your information may be affected. Please note that because we do not collect sensitive personal information like Social Security numbers, this type of sensitive information was not affected by this incident.

What We Are Doing

We take the privacy of personal information seriously, and deeply regret that this incident occurred. We took steps to address this incident promptly after we were alerted to it. We engaged an outside forensic investigation firm to assist us in investigating the incident and remediating the situation by removing the malware and enhancing the security of all Rain Bird store websites. Upon learning that malicious software may have been affecting Rain Bird's websites on September 15, 2017, we took all of our store websites offline to ensure that no further payments would be processed through those pages. While we are continuing to review and enhance security measures, the incident has now been contained. In addition, we reported the incident to federal law enforcement and will cooperate with their investigation.

We have secured the services of Kroll to provide 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.

Visit **kroll.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **February 2, 2018** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-210-8118. Additional information describing your services is included with this letter.

Your identity monitoring services include the following:

- **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'll receive an alert.
- **Quick Cash Scan:** Quick Cash Scan monitors short-term and cash-advance loan sources. You'll 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

What You Can Do

You can carefully review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card as well as the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

Although Social Security numbers were not at risk in this incident, as a general practice you can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. As an additional precaution, we are providing information and resources to help individuals protect their identities. This includes an "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information

For more information about this incident, or if you have additional questions or concerns about this incident, please call 1-833-210-8118, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready. Again, we sincerely regret any concern this event may cause you.

Sincerely,

Rain Bird Corporation

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

Information about Identity Theft Protection

Review Accounts and Credit Reports: You should 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 at the bottom of this page.

You should also 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/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: 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, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: 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 Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

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 at least 90 days. 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. 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. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity;

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and

(4) payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

More Information about Fraud Alerts and Credit Freezes: 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:
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374

Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

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:
P.O. Box 105281
Atlanta, GA 30348
877-322-8228

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872