



October 27, 2023

BY EMAIL

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: Resort Data Processing, Inc. – Notice of Security Incident

To Whom It May Concern,

I am writing to provide notice of a security event (the “event”) involving Resort Data Processing, Inc. (“RDP”). RDP is making this notification on behalf of all affected clients, including those clients set forth in Exhibit A whose number of affected state residents exceeds the statutory reporting threshold to your office. By providing this notice, RDP does not waive any rights or defenses regarding the applicability of state or federal law or personal jurisdiction.

On August 21, 2023, RDP learned of a SQL injection vulnerability to redirect payment card information from in-process transactions on our clients’ on-premises Internet Reservation Module (“IRM”) servers. Once the vulnerability was discovered, RDP immediately took steps to deploy a security patch and additional safeguards onto its systems and initiated an investigation with the assistance of a leading cybersecurity firm. RDP also notified law enforcement. On August 23, 2023, the unauthorized activity was contained. This vulnerability does not impact RDP’s systems.

RDP notified affected clients. The event affected the personal information of 186 Maryland residents across the clients listed in Exhibit A. The types of affected personal information included name, mailing address, email address, and credit card information. RDP anticipates notifying all affected individuals on behalf of all affected clients beginning on October 27, 2023.

RDP is offering these individuals 12 months of complimentary credit monitoring and identity restoration services through Kroll Inc. on behalf of all clients. This includes single bureau credit monitoring, fraud consultation, and identity theft restoration if any individual becomes a victim of identity theft. A copy of the consumer notice is also attached.

RDP takes security seriously and is actively strengthening its security measures, including by enhancing its secure software development lifecycle and monitoring.

Orrick, Herrington & Sutcliffe LLP

401 Union Street
Suite 3300
Seattle, WA 98101-2668

+1 206 839 4300

orrick.com

Joseph C Santiesteban

E jsantiesteban@orrick.com
D +1 206 839 4352
F +1 206 839 4301



The information submitted herein is proprietary and confidential and should be afforded confidential treatment. If you have any questions, please do not hesitate to contact me at +1 (408) 772-0709 or at jsantiesteban@orrick.com.

Respectfully yours,

/s/ Joseph C. Santiesteban
Partner, Orrick Herrington & Sutcliffe LLP

Exhibit A

Maryland

Alta's Rustler Lodge	5 residents
Bluefin Bay Resort	8 residents
Campland on the Bay	4 residents
Dover House Condominium Association Timeshare Resort and Vacation Rental	9 residents
Franciscan Lakeside Lodge by Granlibakken	2 residents
Granlibakken Tahoe	4 residents
Hidden Mountain Resort	43 residents
Mark Spencer Hotel	7 residents
Odyssey Resorts	9 residents
Roche Harbor Resort	5 residents
Silver Cloud Hotel - Tacoma Waterfront	2 residents
Silver Cloud Hotel Seattle - Lake Union	8 residents
Silver Cloud Hotel Seattle - University District	8 residents
Silver Cloud Hotel Tacoma at Point Ruston Waterfront	7 residents
Sunrise Beach Villas	3 residents
Tan-Tar-A Estates	1 resident
The Flanders Hotel	34 residents
The Homestead Resort	5 residents
The Mountain Club on Loon Resort & Spa	11 residents
The Wren at Vail by EastWest Hospitality	1 resident
Villas By The Sea Resort & Conference Center	8 residents
Wilderness Hotel & Golf Resort	2 residents



Re: Notice of Data Breach

Dear {{User.UserAttributes.FirstName}} {{User.UserAttributes.LastName}},

Resort Data Processing ("RDP"), which provides property management software to hotels and real estate businesses, recently experienced a security event that affected your personal information. Please read this notice carefully as it provides up-to-date information on what happened and what we are doing, as well as how you can obtain complimentary identity monitoring services.

What happened?

RDP recently learned that an unauthorized actor used a vulnerability in our reservation booking application at some of our customers' locations to download payment card information. Once we identified the issue, we began rolling out a software update that remediated the vulnerability. We have since issued additional software updates to further strengthen the security of our application and implemented additional monitoring. A forensic firm has been engaged to investigate what happened and what data may have been affected. We also notified law enforcement. No RDP systems were impacted.

What information was involved?

We determined on September 22, 2023, that your name, payment card number ending in {{User.UserAttributes.ImpactedData1}}{{User.UserAttributes.ImpactedData2}}{{User.UserAttributes.ImpactedData3}}, expiration date, and CVV were acquired by an unauthorized actor sometime between August 2022 and mid-August 2023.

This security event did not impact your Social Security number, state identification number, or bank account information.

What we are doing:

RDP is committed to safeguarding personal information. RDP is offering one year of complimentary identity monitoring services through our preferred third-party vendor, Kroll, where those services are available. 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, Fraud Consultation, and Identity Theft Restoration.

Please see [Attachment A](#) for details regarding these complimentary identity monitoring services, as well as how to activate.

In addition to these actions, RDP has taken additional steps to deploy additional safeguards onto our systems, including reinforcing our security practices and is actively reviewing our systems to enhance security monitoring and controls, and to fortify the same. And, as part of our ongoing security operations, we regularly review our security and privacy policies and procedures and implement changes when needed to enhance our information security and privacy programs and controls.

What you can do:

In addition to activating the identity monitoring services being offered to you at no charge, we encourage you to take the following precautions:

- It is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police. Additional information about how to help protect your identity is contained in [Attachment B](#).

For more information:

RDP has established a dedicated call center to answer questions about the security event as well as the Kroll services that we are offering to you. If you have any questions, please call the call center at 866-726-7240 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

We regret any inconvenience that this security event may have caused you, and we remain committed to safeguarding personal information.

Sincerely,

A handwritten signature in black ink, appearing to read 'Matt LaDuke', is written over a light blue horizontal line.

Matt LaDuke
Resort Data Processing, Director of Operations



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until **{{User.UserAttributes.ActivationDeadline}}** to activate your identity monitoring services.*

Membership Number: **{{User.UserAttributes.MembershipNumber}}**

Zip Code: **{{User.UserAttributes.ZipCode}}**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

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'll 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, assisting 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.

Attachment B

MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax

Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
(888) 766-0008
www.equifax.com

Experian

Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

TransUnion LLC
P.O. Box 2000
Chester, PA 190222000
(800) 680-7289
www.transunion.com

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

1. Your 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 those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

District of Columbia Residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov, and www.oag.dc.gov.

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

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

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

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-566-7226 (Toll-free within North Carolina); +1 (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, +1 (800)-771-7755; or www.ag.ny.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9392 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, RI 02903; +1 (401) 274-4400; or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia Residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).