



March 20, 2025

By Email
Office of the Attorney General
Idtheft@oag.state.md.us

Orrick, Herrington & Sutcliffe LLP
401 Union St
Suite 3300
Seattle, WA 98101

+1 206-839-4300
orrick.com

RE: Notice of Security Event | Resort Data Processing

Joseph Santiesteban

Dear Attorney General:

E JSantiesteban@orrick.com
D +1 206-839-4300
F +1 206-839-4301

We are writing on behalf of our client, Resort Data Processing ("The Company"), which provides property management software to hotels and real estate businesses, to notify you of a security event. The Company recently identified evidence that an unauthorized actor was able to use compromised vendor credentials to scrape information that was entered by individuals making internet reservations at a customer location between December 25, 2024 and January 22, 2025. The Company took steps to stop it and engage a forensic firm to investigate what happened and what data may have been affected.

Following a review of the event, the Company determined that the personal information associated with 3 Maryland residents was affected. The types of personal information that could have been scraped include name, payment card number, CVV, and expiration date.

The Company is committed to safeguarding personal information. The Company has taken additional steps to deploy additional safeguards onto its systems, including reinforcing security practices and is actively reviewing its systems to enhance security monitoring and controls, and to fortify the same. And, as part of its ongoing security operations, The Company regularly reviews its security and privacy policies and procedures and implements changes when needed to enhance its information security and privacy programs and controls.

The Company began notifying Maryland residents via U.S. postal mail on March 20, 2025 and is offering one year of complimentary credit monitoring and identity restoration services through its preferred third-party vendor, Kroll, where those services are available. A sample notice is attached.

If your office requires any further information in this matter, please contact me at 206-839-4300 or JSantiesteban@orrick.com.

Sincerely,
Joseph Santiesteban
Partner
Orrick, Herrington, & Sutcliffe, LLP

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

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

Re: Notice of Data Breach

Dear <<first_name>> <<last_name>>,

Resort Data Processing (“RDP”), which provides property management software to hotels and real estate businesses, recently identified 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 credit monitoring and identity restoration services.

What happened?

RDP recently identified evidence that an unauthorized actor was able to use compromised vendor credentials to scrape information that was entered by individuals making internet reservations at a customer location. Once we identified the issue, we took steps to stop it and engage a forensic firm to investigate what happened and what data may have been affected.

What information was involved?

We recently determined that your name, payment card number ending in <<b2b_text_1 (data elements)>>, CVV, and expiration date likely were scraped by an unauthorized actor between December 25, 2024 and January 22, 2025.

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 also offering one year of complimentary credit monitoring and identity restoration services through our preferred third-party vendor, Kroll, where those services are available.

Please see [Attachment A](#) for details regarding these complimentary credit monitoring and identity restoration services, as well as how to enroll with your unique code. **You must enroll by <<b2b_text_6 (activation deadline)>> to receive these services.**

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 enrolling in the credit monitoring and identity restoration 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 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, (866) 686-2170, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

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

Sincerely,

Matt LaDuke

Resort Data Processing, Director of Operations



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

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

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

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, 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.

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 tollfree (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 19022-2000
(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 governmentissued 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 (<https://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 <https://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, Rhode Island 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).