ZERODAY LAW

VIA EMAIL & FEDEX

July 23, 2021

Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
1050 E Interstate Avenue
Suite 200 Bismarck, ND 58503-5574
Email: ndag@nd.gov

Re: *Notice of Data Security Event Relating to North Dakota Residents*

To Whom It May Concern:

By this letter, I am providing notice on behalf of Resort Data Processing, Inc. ("RDP"), a property management software provider, in connection with a data security event involving its online booking engine used by hotels and resorts that involved the personal information of residents of North Dakota.

On approximately June 14, 2021, RDP discovered that its online booking engine was the victim of a cybersecurity attack in which attackers obtained credit/debit card information for some guests. Upon learning of the cyberattack, RDP took immediate steps to terminate the attackers' access and developed and deployed a security patch. Additionally, a leading cybersecurity forensics firm was hired to fully investigate the incident. We understand this malicious activity occurred between approximately February 22, 2021 and approximately June 14, 2021 and for one customer, between approximately January 2019 and approximately May 2019.Please find enclosed a copy of the written notices being sent to twenty-nine (29) North Dakota residents via mail on July 23, 2021. Should you have any questions I can be reached at the number below or via email at tara@zerodaylaw.com.

Sincerely,

Tara Swaminatha
Principal

Encl.

211560

R E S O R T
DATA PROCESSING
c/o Havit
200 South Chestnut Street
Elizabethtown, PA 17022

<<ccName>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

July 23, 2021

Dear <<ccName>>,

We are writing you on behalf of Resort Data Processing, Inc., a property management software provider, to inform you of a recent cybersecurity attack against our online booking system used by hotels and resorts. The incident may have involved your personal information, including your name and credit or debit card information. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources available to help you.

What Happened: On or about June 14, 2021, we became aware of suspicious activity related to our online booking system. We took immediate steps to terminate the attackers' access and developed and deployed a security patch. We enlisted a leading cybersecurity forensics firm to assist us in fully investigating the incident. The investigation revealed that attackers used malicious code to acquire credit/debit card information entered while booking reservations at properties that use our online booking system. The investigation identified malicious activity between approximately February 22, 2021 and approximately June 14, 2021 along with compromised credit/debit card information from reservations made between approximately February 22, 2021 and approximately June 14, 2021. Additionally, malicious activity was identified for one customer beginning on or about January 2019 along with compromised credit/debit card information from reservations made between approximately January 31, 2019 and approximately May 28, 2019.

Who and What Information Was Involved: If you are receiving this letter, your payment card was likely involved in the incident for reservations made online directly with a hotel or resort between February 22, 2021 and June 14, 2021. You may call the number below for more information. Information at risk may have included your name, address, email address, credit/debit card number, expiration date, and security code/card verification code. No bookings were affected.

What We Are Doing: We are taking steps to help prevent this type of incident from occurring in the future. Since the incident, we fixed the software vulnerability and are consulting with cybersecurity experts to identify and implement additional controls to further enhance our online booking system's security.

What You Can Do: You should carefully review the credit and debit card statements for any payment cards you have used to make an online reservation. If you identify any suspicious activity, immediately contact your financial institution.

More Information: We have set-up a toll-free number you may call with questions. Call center operators will be available at 866-991-0648 Monday through Friday from 9AM – 9 PM Eastern Time. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

William Csete

Bill Csete
CTO

Recommended Steps to Help Protect Your Credit Card Information

Three Major Credit Bureaus	**Equifax**: 1-866-349-5191, PO Box 105069, Atlanta, GA 30348, www.equifax.com **Experian**: 1-888-397-3742, PO Box 9554, Allen, TX 75013, www.experian.com **TransUnion**: 1-800-680-7289, PO Box 2000, Chester, PA 19022, www.transunion.com

1. Review your CREDIT REPORTS. We recommend you remain vigilant for fraud and identity theft by reviewing account statements and monitoring free credit reports. Under federal law, every 12 months you are entitled to a **free** copy of your credit report from each of the 3 major credit bureaus - go to: www.annualcreditreport.com or call 1-877-322-8228. Otherwise, fees may be required to be paid to the credit reporting agencies. You may stagger your requests so that you receive a free report from 1 of the 3 credit bureaus every 4 months.

2. Right to obtain/file police reports. A police report might be required to dispute fraud. You have the right to obtain and/or file a police report if you experience identity fraud. You may have to provide some proof that you were a victim of identity theft. You can report suspected identity theft to local law enforcement or to your state Attorney General, which you can find here: https://www.naag.org/find-my-ag/.

3. Place FRAUD ALERTS and obtain information about fraud alerts from the 3 credit bureaus. Place a fraud alert at 1 of the 3 major credit bureaus by phone or online; this tells creditors to follow certain procedures, e.g., contacting you, before opening any new accounts in your name or changing existing accounts. Please Note: A fraud alert can protect you but may delay you obtaining credit. To place a fraud alert, **notify one of the credit bureaus** and they will notify the others. You will receive confirmation letters and then can order all 3 credit reports, free of charge. An initial fraud alert lasts 1 year. **Note: No one may place a fraud alert on your credit report except you.**

4. Place a SECURITY FREEZE. By placing a security freeze, no one will be able to use your identifying information to open new accounts or borrow money in your name. **Contact all 3 credit bureaus** listed above to place the security freeze. Please Note: When you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you lift or permanently remove the freeze. Placing and removing credit freezes is free.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. Identity Theft Clearinghouse, FTC, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft or www.ftc.gov, 1-877-438-4338, TTY: 1-866-653-4261.

Iowa Residents: You can report suspected identity theft to local law enforcement or to: Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 515-281-5926, www.iowaattorneygeneral.gov www.iowaattorneygeneral.gov.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New York Residents: Office of the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Personal information of fifteen Rhode Island residents was impacted.

South Carolina Residents: You can obtain additional information about the steps you can take to avoid identity theft from South Carolina Department of Consumer Affairs at 1-800-922-1594.

R E S O R T
DATA PROCESSING
c/o Havit
200 South Chestnut Street
Elizabethtown, PA 17022

<<ccName>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

July 23, 2021

Dear <<ccName>>,

We are writing you on behalf of Resort Data Processing, Inc., a property management software provider, to inform you of a recent cybersecurity attack against our online booking system used by hotels and resorts. The incident may have involved your personal information, including your name and credit or debit card information. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources available to help you.

What Happened: On or about June 14, 2021, we became aware of suspicious activity related to our online booking system. We took immediate steps to terminate the attackers' access and developed and deployed a security patch. We enlisted a leading cybersecurity forensics firm to assist us in fully investigating the incident. The investigation revealed that attackers used malicious code to acquire credit/debit card information entered while booking reservations at properties that use our online booking system. The investigation identified malicious activity as early as January 2019 along with compromised credit/debit card information from reservations made between approximately January 31, 2019 and approximately May 28, 2019 and also between approximately February 22, 2021 and June 14, 2021.

Who and What Information Was Involved: If you are receiving this letter, your payment card was likely involved in the incident for reservations made online directly with a hotel or resort between approximately January 31, 2019 and approximately May 28, 2019. You may call the number below for more information. Information at risk may have included your name, address, phone number, email address, credit/debit card number, expiration date, and security code/card verification code. No bookings were affected.

What We Are Doing: We are taking steps to help prevent this type of incident from occurring in the future. Since the incident, we fixed the software vulnerability and are consulting with cybersecurity experts to identify and implement additional controls to further enhance our online booking system's security.

What You Can Do: You should carefully review the credit and debit card statements for any payment cards you have used to make an online reservation. If you identify any suspicious activity, immediately contact your financial institution.

More Information: We have set-up a toll-free number you may call with questions. Call center operators will be available at 866-991-0648 Monday through Friday from 9AM – 9 PM Eastern Time. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

William Csete

Bill Csete
CTO

Recommended Steps to Help Protect Your Credit Card Information

Three Major Credit Bureaus	**Equifax**: 1-866-349-5191, PO Box 105069, Atlanta, GA 30348, www.equifax.com **Experian**: 1-888-397-3742, PO Box 9554, Allen, TX 75013, www.experian.com **TransUnion**: 1-800-680-7289, PO Box 2000, Chester, PA 19022, www.transunion.com

1. Review your CREDIT REPORTS. We recommend you remain vigilant for fraud and identity theft by reviewing account statements and monitoring free credit reports. Under federal law, every 12 months you are entitled to a **free** copy of your credit report from each of the 3 major credit bureaus - go to: www.annualcreditreport.com or call 1-877-322-8228. Otherwise, fees may be required to be paid to the credit reporting agencies. You may stagger your requests so that you receive a free report from 1 of the 3 credit bureaus every 4 months.

2. Right to obtain/file police reports. A police report might be required to dispute fraud. You have the right to obtain and/or file a police report if you experience identity fraud. You may have to provide some proof that you were a victim of identity theft. You can report suspected identity theft to local law enforcement or to your state Attorney General, which you can find here: https://www.naag.org/find-my-ag/.

3. Place FRAUD ALERTS and obtain information about fraud alerts from the 3 credit bureaus. Place a fraud alert at 1 of the 3 major credit bureaus by phone or online; this tells creditors to follow certain procedures, e.g., contacting you, before opening any new accounts in your name or changing existing accounts. Please Note: A fraud alert can protect you but may delay you obtaining credit. To place a fraud alert, **notify one of the credit bureaus** and they will notify the others. You will receive confirmation letters and then can order all 3 credit reports, free of charge. An initial fraud alert lasts 1 year. **Note: No one may place a fraud alert on your credit report except you.**

4. Place a SECURITY FREEZE. By placing a security freeze, no one will be able to use your identifying information to open new accounts or borrow money in your name. **Contact all 3 credit bureaus** listed above to place the security freeze. Please Note: When you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you lift or permanently remove the freeze. Placing and removing credit freezes is free.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. Identity Theft Clearinghouse, FTC, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft or www.ftc.gov, 1-877-438-4338, TTY: 1-866-653-4261.

Iowa Residents: You can report suspected identity theft to local law enforcement or to: Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 515-281-5926, www.iowaattorneygeneral.gov www.iowaattorneygeneral.gov.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New York Residents: Office of the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Personal information of fifteen Rhode Island residents was impacted.

South Carolina Residents: You can obtain additional information about the steps you can take to avoid identity theft from South Carolina Department of Consumer Affairs at 1-800-922-1594.