WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

May 4, 2020

Anjali Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

VIA EMAIL: consumer@ag.iowa.gov

Attorney General Tom Miller
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Data Security Incident

Dear Attorney General Miller:

We represent Informatics, Inc. ("Informatics"), the website host of www.mycountyparks.com, a website maintained by Iowa's County Conservation System ("ICCS"), with respect to a data security incident (hereinafter, the "Incident") described in more detail below. Informatics and ICCS take the security and privacy of the information in their control seriously, and have taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On April 4, 2020 ICCS was first alerted to feedback received from several ICCS website users who discovered that fraudulent purchases were made on their payment cards after using the www.mycountyparks.com website. ICCS then quickly informed Informatics, Inc., the host of www.mycountyparks.com to investigate.

On April 9, 2020, Informatics alerted ICCS that a technical investigation performed by Informatics revealed previously undiscovered evidence that an unknown individual had placed a malicious code on www.mycountyparks.com as early as January 31, 2020. The malicious code was used to intercept payment card information of www.mycountyparks.com website users who made purchases on the website between the dates of January 31, 2020 and April 8, 2020. Upon discovery, steps were taken to swiftly secure the ICCS website, such as the removal of the malicious code.

At this time, ICCS and Informatics have no evidence to indicate that the attacker responsible for the attack may have viewed or otherwise acquired any personal information of consumers affected by this incident other than their name, address, and payment card information.

2. Number of Iowa residents affected.

Two thousand five hundred eighty (2,580) Iowa residents were potentially affected by this security incident. An incident notification letter addressed to these individuals was mailed on May 4, 2020, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

Informatics and ICCS have taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of potentially impacted individuals' information. Those steps include strengthening its cybersecurity posture, such as removal of the malicious code that caused the Incident, and providing potentially impacted individuals with timely notice of the Incident and complimentary identity theft restoration and credit monitoring services for a period of twelve (12) months.

4. Contact information.

Informatics and ICCS remains dedicated to protecting the sensitive information in their control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@wilsonelser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure

Iowa's County Conservation System

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

We are writing to inform you of a data security incident involving www.mycountyparks.com, a website maintained by Iowa's County Conservation System ("ICCS"), which may have resulted in the disclosure of your name, address, and payment card information. We take the security of your personal information very seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident, steps you can take to protect your information, and resources we are making available to help you.

On April 4, 2020 ICCS was first alerted to feedback received from several ICCS website users who discovered that fraudulent purchases were made on their payment cards after using the www.mycountyparks.com website. ICCS then quickly informed the host of www.mycountyparks.com to investigate.

On April 9, 2020, the host of the www.mycountyparks.com alerted ICCS that a technical investigation performed by the website host revealed previously undiscovered evidence that an unknown individual had placed a malicious code on www.mycountyparks.com as early as January 31, 2020. The malicious code was used to intercept payment card information of www.mycountyparks.com website users who made purchases on the website between the dates of January 31, 2020 and April 8, 2020. Upon discovery, steps were taken to swiftly secure the ICCS website, such as the removal of the malicious code.

At this time, ICCS has no evidence to indicate that the attacker responsible for the attack may have viewed or otherwise acquired any personal information other than your name, address, and payment card information. We are committed to ensuring the security of all information in our control, and are taking steps to prevent a similar event from occurring in the future. This includes strengthening our cybersecurity posture.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

To enroll in this service, go to the myTrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Please know that the protection of your personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call (855) 917-3466, Monday – Friday, 9:00am to 9:00pm Eastern Standard Time.

Sincerely,

Thomas F. Hazelton

System Administrator
www.mycountyparks.com
P.O. Box 400
Hiawatha, IA 52233-0400

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina:* It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia:*
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa:*
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon:*
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:
You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.
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
Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903, 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 www.ncdoj.gov
Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224, 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

---

For residents of *Massachusetts:* It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.