Racine County

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: [redacted]

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

March 3, 2020

Re: Notification of Data Security Incident

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident that may have affected your personal information. Racine County ("Racine") takes the privacy and security of the sensitive information in its care very seriously. This is why we are contacting you, offering you complimentary credit monitoring and identity protection services, and informing you about steps you can take to help protect your personal information.

What Happened? On April 25, 2019, we discovered unusual activity in our email system. Upon discovering this activity, we immediately took steps to secure our digital environment and launched an internal investigation. We also engaged an independent forensics firm to determine what happened and whether personal and/or protected health information may have been accessed or acquired without authorization. On July 1, 2019, we learned that certain Racine employee email accounts had been accessed without authorization. Upon completion of the forensic investigation, we engaged a document review vendor to search the contents of the impacted email accounts to identify the individuals whose personal information may have been contained within the accounts. We subsequently learned that messages and/or attachments contained within the impacted email accounts included your personal information. We then worked diligently to identify up-to-date address information in order to notify all potentially impacted individuals. This process was completed on February 7, 2020.

While we are not presently aware of the misuse of any information that may have been involved in this incident, we are providing this letter to you to inform you of the incident and to share steps that you can take to help protect your personal information.

What Information Was Involved? Based on our investigation, the information may include your <<Variable Text>>.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. In addition, we have taken affirmative steps to minimize the likelihood of a similar incident occurring in the future. This includes working with cybersecurity experts to enhance the security of our email environment. We are also providing you with information about steps that you can take to help protect your personal information. As an added precaution, we are offering you MyIDCare™, identity theft protection services through ID Experts®, a data breach and recovery services expert. MyIDCare services include twelve months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. Also, while we are not aware of any evidence that any information has been misused as a result of this incident, as a precautionary measure to safeguard your personal information, we encourage you to enroll in complimentary MyIDCare services by calling 1-800-939-4170 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6:00 am – 5:00 pm Pacific Time. Please note the deadline to enroll is June 3, 2020.

For More Information: We remain committed to protecting the personal information in our care and apologize for any worry or inconvenience this may cause you. If you have any questions, please contact the ID Experts helpline at 1-800-939-4170 or go to https://app.myidcare.com/account-creation/protect, and have your unique code ready to provide to the fraud specialist.

Sincerely,

Michael Lanzdorf
Corporation Counsel | Racine County, Wisconsin

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-800-680-7289	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Kentucky, Maryland, North Carolina, and Oregon can obtain more information from their Attorneys General using the contact information below.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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.

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

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

You also have certain rights under the Fair Credit Reporting Act (FCRA): You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.