



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

To Enroll in MyIDCare, or for Any Questions,
 Please Call:
 1-800-939-4170
 Or Visit: <https://app.myidcare.com/account-creation/protect>
 Enrollment Code for MyIDCare:
 <<XXXXXXXXXX>>

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

April 12, 2019

Subject: Notice of Data Security Incident

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

With the assistance of ID Experts, a data breach response consultant, Dakota County is writing to inform you of a data security incident that may have involved your private information described below. At Dakota County, we take the privacy and security of your information very seriously and strive to maintain your trust through a continued commitment to protecting your information. Although we are not aware at this time that your information has been misused, we want to inform you about steps that can be taken to help protect your private information and to offer identity and credit monitoring services. We are very sorry for any concern that this incident may cause you.

What Happened?

On February 13, 2019, Dakota County discovered unauthorized access to one Dakota County Social Services employee’s email account. Upon learning of this incident, we reset the passwords for all employee email accounts and implemented additional email and network security measures. Dakota County also launched an investigation and engaged independent cybersecurity experts to provide assistance. On March 27, 2019, as a result of this investigation, Dakota County confirmed that emails within the impacted account may have been accessed without authorization and that some of those emails contained your private information.

At this time, Dakota County is not aware that any of your private information potentially involved in this incident has been misused. Nonetheless, as a precaution, we are providing you with access to complimentary identity and credit monitoring services through ID Experts.

What Information Was Involved?

Some of the following private information may have been involved: name, address, driver’s license number, *[social security number,]* health insurance information, and/or medical history, treatment, or diagnoses information. We are not currently aware of any misuse of your information.

What Are We Doing?

Upon learning of this incident, we implemented additional security measures on all employee email accounts and began an investigation into this incident. In addition, to help protect your private information, we are offering identity theft protection services through ID Experts, a data breach and recovery services consultant. Such services, known as MyIDCare, include the following: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What Can I Do?

You can follow the recommendations on the following pages to help protect your private information. In addition, we encourage you to contact ID Experts with any questions and to enroll in the complementary MyIDCare services offered to you by calling 1-800-939-4170 or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code at the top of this letter.

MyIDCare experts are available Monday through Friday from 8 am – 7 pm Central Time. Please note the deadline to enroll is July 12, 2019.

For More Information.

Further information about protecting your private information appears on the following pages. If you have questions or require additional assistance, you may contact MyIDCare experts by calling 1-800-939-4170. Please note that Dakota County is preparing a report describing this incident. You may request a copy of the report by calling 651-554-6244, emailing data.practices@co.dakota.mn.us, or by mailing your request to the following address:

HIPAA Privacy Officer / Data Practices Compliance Official
Dakota County Community Services Administration
1 Mendota Rd W, Suite 500
West St. Paul, MN 55118.

Thank you for your patience as we work through this incident. We take this matter very seriously and do not take your trust for granted. We are very sorry for any worry or inconvenience this may cause you.

Sincerely,



Matt Smith
Dakota County Manager

(Enclosures)



1. Website and Enrollment. Go to <https://app.myidcare.com/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR 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	1-877-322-8228	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 at least 90 days. 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: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. 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. You can obtain more information from their FTC using the contact information below.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <http://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>