haynesboone

July 19, 2019

VIA EMAIL AND FIRST CLASS MAIL

Office of the Attorney General
600 East Boulevard Avenue, Department 125
Bismarck, ND 58505-0040
ndag@nd.gov

Dear Sir or Madam:

We represent Dallas Computer Services, Inc., 500 N. Central Expressway, Suite 280, Plano, TX, 75074 ("DCS"). Pursuant to N.D. Cent. Code § 51-30-02, we write to notify you of an incident that affects the security of personal information relating to two North Dakota residents. By providing this notice, DCS does not waive any rights or defenses regarding the applicability of North Dakota law or personal jurisdiction.

DCS provides information services to its clients, including insurance companies and agents. Its clients use these services to verify information on potential policy holders.

On June 24, 2019, DCS discovered that one of its subscriber's log-in credentials had been compromised and had been used to gain unauthorized access to the records of two North Dakota residents. Access occurred during the early morning hours of June 24, 2019, and DCS learned that the incident impacted North Dakota residents on July 15, 2019. The records that were accessed may have contained an individual's name, address, date of birth, and Texas driver's license or identification card number. The records did not contain social security numbers or financial account information.

There is no indication of a breach of DCS's network security. Instead, it appears that the authorized DCS subscriber failed to properly secure the compromised credentials, in violation of DCS's subscription agreement with the subscriber.

Immediately upon discovering this issue, DCS discontinued access to its information database using the compromised credentials and contacted state law enforcement, which is conducting an investigation. DCS has implemented additional security to help prevent a similar occurrence in the future.

DCS will notify affected individuals by letter, scheduled for delivery July 22, 2019. A sample of the notice letter is attached for your reference. Notice was not delayed as a result of a law enforcement investigation. DCS retained ID Experts® to provide affected individuals with MyIDCare™, which includes 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

Haynes and Boone, LLP
Attorneys and Counselors
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Phone: 214.651.5000
Fax: 214.651.5940
www.haynesboone.com

If you have any questions, please do not hesitate to contact me.

Sincerely,

Timothy A. Newman
Haynes and Boone, LLP
tim.newman@haynesboone.com
Direct Dial 214-651-5029

Enclosure

DCS
INFORMATION SYSTEMS

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE
NAME
ADDRESS1
ADDRESS2
2Dcode CSZ
SEQ COUNTRY
BREAK

To Enroll, Please Call:
833-300-6929
Or Visit: https://ide.myidcare.com/dcs
Enrollment Code:
<<XXXXXXXX>>

<<Mail Date>>

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data security incident experienced by Dallas Computer Services, Inc. ("DCS") that may have resulted in the exposure of your personal information. Your financial account information and Social Security number were not impacted by this incident. We value and respect the privacy of your information, and we 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 we are making available to help you. This notice was not delayed as a result of a law enforcement investigation.

What Happened

DCS provides information services to its clients, including insurance companies and agents. Our clients use our services to verify information on potential policy holders.

On June 24, 2019, we discovered that one of our subscriber's log-in credentials had been compromised and had been used to gain unauthorized access to some individuals' records. Your record was among those likely accessed. There is no indication of a breach of DCS's network security. Instead, it appears that the authorized DCS subscriber failed to properly secure the compromised credentials, in violation of our subscription agreement with the subscriber.

What Information Was Involved

Depending on the individual circumstances, the records that were accessed may have contained a driver's name, address, date of birth, and driver's license or identification card number. The records did not contain social security numbers or financial account information.

What We Are Doing

Immediately upon discovering this issue, we discontinued access to our network using the compromised credentials. We also implemented additional network security to prevent a similar occurrence in the future.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 833-300-6929 or going to https://ide.myidcare.com/dcs and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is October 22, 2019.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 833-300-6929 or go to https://ide.myidcare.com/dcs for assistance or for any additional questions you may have.

Sincerely,

Keith Graves

Keith Graves
Vice President
Dallas Computer Services

MyIDCare

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://ide.myidcare.com/dcs 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 833-300-6929 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.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

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.

New Mexico Residents: 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.

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.