

# BakerHostetler

Baker & Hostetler LLP

45 Rockefeller Plaza  
New York, NY 10111

T 212.589.4200  
F 212.589.4201  
www.bakerlaw.com

Theodore J. Kobus III  
direct dial: 212-271-1504  
tkobus@bakerlaw.com

June 21, 2019

**VIA OVERNIGHT MAIL AND EMAIL (CONSUMER@AG.IOWA.GOV)**

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

*Re: Incident Notification*

Dear Sir or Madam:

I am writing on behalf of our client, Dominion Dental Services, Inc., Dominion National Insurance Company, and Dominion Dental Services USA, Inc., each of which operate under the trade name Dominion National (hereinafter referred to collectively as "Dominion National"). Dominion National is an insurer and administrator of dental and vision benefits. Without waiving any objection to personal jurisdiction or ERISA-preemption, this notice is intended to satisfy obligations for Dominion National, its affiliate health plans, self-funded accounts, and customers, to notify your office about this incident.

On April 24, 2019, through its investigation of an internal alert, Dominion National determined that an unauthorized party may have accessed some of its computer servers. Through its investigation of the internal alert, Dominion National determined that the unauthorized access may have occurred as early as August 25, 2010. After learning of this, Dominion National moved quickly to clean the affected servers. Subsequently, Dominion National undertook a comprehensive review of the data stored or potentially accessible from those computer servers and determined, on June 17, 2019, that the data may include personal information pertaining to 538 participating healthcare providers residing in Iowa. The information varies by individual, but may include names in combination with dates of birth and Social Security numbers. Dominion National has no evidence that any information was in fact accessed, acquired, or misused.

Beginning on June 21, 2019, Dominion National will mail notification letters via United States Postal Service First-Class mail to 538 Iowa residents<sup>1</sup> in accordance with I.C.A. § 715C.2<sup>2</sup>. A copy of the notification letter is enclosed.

---

<sup>1</sup> The addresses are being run through the United States Postal Service's National Change of Address (NCOA) database. Therefore, the number of potentially affected residences in your state may change.

<sup>2</sup> Notice is also being provided to 306 current and former members of Dominion National and 116 current and former members of insurance plans Dominion National administers dental and vision benefits for residing in Iowa, in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 C.F.R. § 164.404).

Consumer Protection Division

June 21, 2019

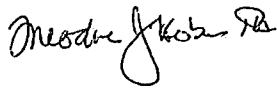
Page 2

Dominion National also posted notice on its website, DominionNational.com, and on DominionNationalFacts.com. Dominion National is also providing a telephone number for potentially affected individuals to call with any questions they may have. Dominion National is offering all potentially affected individuals complimentary two-year memberships to ID Experts® MyIDCare™, which include credit monitoring and fraud protection services.

To help prevent something like this from happening in the future, Dominion National has implemented enhanced monitoring and alerting software. Dominion National also contacted the FBI and will continue to work with them during their investigation.

Please do not hesitate to contact me if you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Theodore J. Kobus III". The signature is written in a cursive style with a prominent "T" and "K".

Theodore J. Kobus III

Enclosure



c/o ID Experts  
 P.O. Box 6336  
 Portland, OR 97228-6336

To Enroll, Please Call:  
 877-503-8923 or TTY/TDD: 844-261-6819  
 Or Visit:  
<https://ide.myidcare.com/dominionnational>  
 Enrollment Code: <<Activation Code>>  
 Expiration Date for Enrollment: November 21, 2019

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

<<Date>>

Dear <<Name 1>>:

Dominion National is committed to protecting the privacy of the information we maintain. We are writing to inform you that we recently identified and addressed a data security incident that may have involved your information. We have no evidence that any of your information was in fact accessed, acquired, or misused, but we want you to know that this incident occurred. This notice explains the incident, measures we have taken, and some steps you may want to take in response.

On April 24, 2019, through our investigation of an internal alert, with the assistance of a leading cyber security firm, we determined that an unauthorized party may have accessed some of our computer servers. The unauthorized access may have occurred as early as August 25, 2010. After learning of this, we moved quickly to clean the affected servers and implement enhanced monitoring and alerting software. We also contacted the FBI and will continue to work with them during their investigation.

We have undertaken a comprehensive review of the data stored or potentially accessible from those computer servers and have determined that the data may include personal information for current and former healthcare providers who provided services to members of dental insurance programs underwritten and/or administered by Dominion National. The information may include your name, date of birth, Social Security number, and/or taxpayer identification number.

As a precaution, we have secured the services of ID Experts® to offer you a complimentary two-year membership to ID Experts MyIDCare™, which includes credit monitoring and fraud protection services. MyIDCare is completely free to you and enrolling in this program will not hurt your credit score. For more information on MyIDCare, including instructions on how to activate your complimentary two-year membership, as well as some additional steps you can take in response to this incident, please see the pages that follow this letter.

We encourage you to remain vigilant for incidents of fraud by monitoring your financial account statements. If you see charges or activity you did not authorize, please contact your financial institution immediately.

We regret any inconvenience or concern this may cause you. We are committed to improving and maintaining your confidence in us. If you have any questions, please visit our website at [DominionNationalFacts.com](http://DominionNationalFacts.com) or call our dedicated incident response line at 877-503-8923. TTY/TDD users can call 844-261-6819. The dedicated incident response line is open Monday through Friday, 8:00 a.m. to 8:00 p.m., Eastern Time.

Sincerely,

Mike Davis  
 President

## **MYIDCARE ENROLLMENT INFORMATION**

**1. Website and Enrollment.** Go to <https://ide.myidcare.com/dominionnational> 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 to use this service. If you need assistance, MyIDCare will be able to assist you.

**3. Telephone.** Contact MyIDCare at 877-503-8923 or TTY/TDD: 844-261-6819 to enroll in MyIDCare, gain additional information about this incident, and speak with knowledgeable representatives about steps you can take in response.

If you discover any suspicious items and have enrolled in MyIDCare, notify MyIDCare immediately by calling 877-503-8923 or TTY/TDD: 844-261-6819, 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.

## **ADDITIONAL STEPS YOU CAN TAKE**

Regardless of whether you choose to take advantage of the complimentary credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Centre, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**If you are a resident of Connecticut, Maryland, or North Carolina**, you may contact and obtain information from your state attorney general at:

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag)
- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 (toll-free within Maryland) / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us)
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)

**If you are a resident of West Virginia**, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company.

For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under FCRA.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights

For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.