July 16, 2024

Brian H. Myers
(202) 626-7695 (direct)
Brian.Myers@WilsonElser.com

Via Email:

Office of the Attorney General
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319
consumer@ag.iowa.gov

Re: Notice of Cybersecurity Incident

Office of the Attorney General:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents FCDG Management, LLC dba First Choice Dental, located at 440 Science Drive, Suite 110 in Madison, Wisconsin 53711, and we are providing notice of a recent cybersecurity incident (hereinafter, the "Incident"). By providing this notice, FCD does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

This letter will serve to inform you of the nature of the Incident, what information may have been involved, and the steps that FCD has taken in response to the Incident. We have also enclosed hereto a sample copy of the notice letter we recently mailed to the individuals whose personal information was involved on July 16, 2024.

1. Nature of the Incident

On October 22, 2023, FCD detected a ransomware event on its network, whereby an unauthorized actor gained access to FCD's network, encrypted some of FCD's data, and attempted to extort a ransom payment. Upon discovery of this event, FCD immediately disconnected access to its network and engaged cybersecurity professionals to help secure FCD's network and conduct a forensic investigation.

FCD's forensic investigation found evidence that the unauthorized actor had access to certain FCD files. Upon learning of this, FCD began an extensive and comprehensive review of the files to identify and notify any individuals whose personal information may have been included in those files.

On December 21, 2023, while FCD's review was ongoing, FCD posted a notice of the event on its website, notified the U.S. Department for Health and Human Services, and issued a media notice with the Wisconsin State Journal.

In May 2024, FCD completed its comprehensive review of the data and began preparations to mail personalized notice letters to the individuals whose personal information may have been accessed.

2. Number of individuals and information involved.

FCD's investigation determined that the personal information of 1,284 Iowa residents was involved. While the information involved varies for each individual, FCD's investigation determined that the unauthorized actor may have had access to files containing the following categories of information: name, date of birth, Social Security number, passport number, driver's license number, government identification number, credit/debit card number, financial account number, and health information. Again, the information involved varies for each individual, and not every category applies in each individual case.

3. Steps taken in response to the Incident.

Data privacy and security are among FCD's highest priorities. Once it discovered the event, FCD moved quickly to secure its systems. Specifically, FCD added new intrusion detection and response tools; enhanced its data backup systems; upgraded its firewall; implemented additional multi-factor authentication requirements for network access; reset passwords and enhanced its password policy; and made additional changes to our network access policies. FCD also engaged specialized cybersecurity professionals to conduct a forensic investigation to determine the nature and scope of the event. FCD will continue to take steps to enhance the security of its network.

In addition, the personalized notification letters that FCD mailed on July 16, 2024 include an offer of complimentary credit monitoring and identity theft protection services for twelve months, along with instructions on how to enroll in those services.

4. Contact information

If you have any questions or need additional information, please do not hesitate to contact me at Brian.Myers@WilsonElser.com or (202) 626-7695.

Regards,

Wilson Elser Moskowitz Edelman & Dicker LLP

Brian H. Myers, Esq.
Certified Information Privacy Professional, United States (CIPP/US)

Encl.

-*- Demonstration Powered by OpenText Exstream 07/12/2024, Version 16.4.0 64-bit -*-

First Choice Dental
c/o Cyberscout, a TransUnion company
PO Box 1286
Dearborn, MI 48120-9998

Via First-Class Mail

P
[redacted]

July 16, 2024

000010103G0400

P

Re: NOTICE OF DATA SECURITY INCIDENT

Dear [redacted],

First Choice Dental ("FCD") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. This letter provides you with information about the incident and the steps we are taking in response, as well as resources you can use to help you protect against the potential misuse of your information.

While we do not have any evidence that anyone's personal information has been misused for identity theft or fraud in connection with this incident, we are offering free credit monitoring and identity theft protection services and this letter includes instructions on how to enroll in those services.

What Happened?

On October 22, 2023, FCD detected it was the target of a ransomware attack, whereby an unauthorized third party gained access to FCD's network, encrypted some of FCD's data, and left a ransom note on FCD's network. Upon discovery of this incident, FCD immediately disconnected access to its network and engaged cybersecurity professionals to help secure FCD's network and conduct a forensic investigation.

FCD's forensic investigation found evidence that some FCD files were accessed by the unauthorized actor. Upon learning of this, FCD began an extensive and comprehensive review of the files to identify and notify any individuals whose personal information may have been accessed.

On December 21, 2023, while FCD's review was ongoing, FCD posted a notice of the incident on its website and issued a media notice with the Wisconsin State Journal.

On May 1, 2024, FCD completed its comprehensive review of the data and began preparations to mail personalized notice letters to the individuals whose personal information may have been accessed.

What Information Was Involved?

Based on our investigation, the unauthorized actor may have accessed the following categories of your personal information: [redacted].

FCD does not have any evidence that the unauthorized actor has misused anyone's personal information for identity theft or fraud in connection with this incident. Based on the information available to us at this time, it appears that the unauthorized actor's primary motivation was to extort a ransom payment from FCD.

-*- Demonstration Powered by OpenText Exstream 07/12/2024, Version 16.4.0 64-bit -*-

What We Are Doing

Data privacy and security is among FCD's highest priorities. Since the discovery of the incident, FCD moved quickly to secure our systems. Specifically, FCD added new intrusion detection and response tools; enhanced our data backup systems; upgraded our firewall; implemented additional multi-factor authentication requirements for network access; reset passwords and enhanced our password policy; and made additional changes to our network access policies. FCD also engaged specialized cybersecurity professionals to conduct a forensic investigation to determine the nature and scope of the Incident. FCD will continue to take steps to mitigate the risk of future harm.

In light of the incident, we are also providing you with access to credit monitoring services. Upon your completion of the enrollment process you will have access to monitoring of your TransUnion credit file as well as a TransUnion credit report and credit score at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, and monitoring your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and consider placing a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information* to learn more.

We also encourage you to enroll in the credit monitoring and identity theft protection services we are making available to you at no cost. The deadline to enroll is October 10, 2024.

To enroll in Credit Monitoring services at no charge, please log on to **www.mytrueidentity.com** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information

If you have any questions or concerns not addressed in this letter, please call 1-833-531-3380 (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Time (excluding U.S. national holidays).

Sincerely,

Jennifer Spink
Vice President of Finance
First Choice Dental Group Management

-*- Demonstration Powered by OpenText Exstream 07/12/2024, Version 16.4.0 64-bit -*-

Steps You Can Take to Help Protect Your Information

Credit Reports: 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.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

P 00001020380000

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You 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. 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:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

This notice was not delayed as a result of any law enforcement investigation.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, you have the right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at 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.

-*- Demonstration Powered by OpenText Exstream 07/12/2024, Version 16.4.0 64-bit -*-

For New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

For Oregon residents, you are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For Rhode Island residents, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

P 0000103030000

-*- Demonstration Powered by OpenText Exstream 07/12/2024, Version 16.4.0 64-bit -*-