dentalcenter
of northwest ohio

<<Date>> (Format: Month Day, Year)

Guardian of
<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear Guardian of <<MemberFirstName>> <<MemberLastName>>,

Dental Center of Northwest Ohio (the "Dental Center") writes to make you aware of a recent incident that may affect the privacy of some of your minor dependent's personal information. While there is currently no evidence that your minor dependent's information has been misused, we are making you aware of the event, the steps we are taking in response, and steps you may take to better protect against possible misuse of your minor dependent's personal information, should you feel it appropriate to do so.

What Happened? On or about September 1, 2018, the Dental Center's IT vendor, Arakyta, made the Dental Center aware of an issue, at Arakyta, potentially impacting certain Dental Center systems. Arakyta later confirmed ransomware had infected Arakyta systems resulting in a disruption to systems storing Dental Center information. The Dental Center immediately launched an investigation into the nature and scope of incident, including working with third-party computer experts to determine what, if any, Dental Center information was impacted by the Arakyta event. Based on the information provided from Arakyta, on November 7, 2018, the Dental Center confirmed that systems containing Dental Center data were potentially accessible to an unknown actor from August 16, 2018 through September 18, 2018. Although the Dental Center has not received reports of actual access to Dental Center data as a result of the Arakyta event, because the Dental Center was unable to rule out the possibility of such access, the Dental Center is notifying individuals whose information was stored on systems potentially impacted by the Arakyta event.

What Information Was Involved? Through the ongoing investigation, the Dental Center determined that the personal information present on systems impacted by the Arakyta event may include your minor dependent's <<ClientDef1>><<ClientDef2>>(name, address, [and insert all applicable data elements]). To date, the Dental Center has not received any reports of actual or attempted misuse of your minor dependent's personal information as a result of the Arakyta event.

What We Are Doing. The Dental Center takes the confidentiality, privacy, and security of information in our care very seriously. Upon learning of the Arakyta event, we immediately commenced an investigation to confirm the nature and scope of the incident as it relates to Dental Center data. We took steps to identify the personal information stored on systems disrupted by the Arakyta event and we are notifying the individuals who are potentially affected. While the Dental Center has security measures in place to protect information in our care, we are taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security. We are also notifying relevant regulators of the Arakyta event.

As an added precaution, the Dental Center is providing you with access to twelve months (12) of Fraud Consultation and Identity Theft Restoration services from Kroll at no cost to you. A description of services can be found within the enclosed *Steps You Can Take to Protect Personal Information*.

What You Can Do. On your minor dependent's behalf, you can review the enclosed *Steps You Can Take to Protect Personal Information*.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have questions or concerns, please call our dedicated hotline at 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Please know Dental Center takes the privacy and security of the patient information in our care very seriously and we sincerely regret any inconvenience or concern this incident may cause you and your minor dependent.

Sincerely,

Melinda Cree
Executive Director
Dental Center of Northwest Ohio

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Kroll Fraud Consultation and Identity Theft Restoration

While, to date, the investigation found no evidence that data potentially affected by this incident has been misused, in an abundance of caution, we are offering you access to Fraud Consultation and Identity Theft Restoration at no cost to you for one year through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Your child's Membership Number is: **<<Member ID>>**

Additional information describing your child's services is included with this letter.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your minor's dependent's account statements and credit reports, if such exist, for suspicious activity. Typically, a minor under the age of eighteen does not have credit in his or her name, and the consumer reporting agencies do not have a credit report in a minor's name; however, below are steps an individual can take to better protect his or her personal information, if a credit report has been issued in the individual's name:

Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of your credit report.

Individuals have the 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 their expressed authorization. The security freeze is designed to prevent credit, loans, and services from being approved in individual's names without their consent. However, individuals should be aware that using a security freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, individuals cannot be charged to place or lift a security freeze on Their credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/credit-freeze	PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifacx.com/personal/credit-report-services

In order to request a security freeze, individuals will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If individual have moved in the past five (5) years, provide the addresses where individual has 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 individual was a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, individuals have the right to place an initial or extended "fraud alert" on their file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If individuals are a victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should individuals wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

Although we have no reason to believe that your minor dependent's personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your dependent's name and what to do if they become a become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect your dependent, 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. You have the right to file a police report on your dependent's behalf, if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to promptly to law enforcement. This notice has not been delayed by law enforcement.

For 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 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. We encourage you to 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.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident.

TAKE ADVANTAGE OF FRAUD CONSULTATION AND IDENTITY THEFT RESTORATION SERVICES

You've been provided with access to the following services from Kroll:

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your minor dependent's identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If your minor dependent becomes a victim of identity theft, an experienced Kroll licensed investigator will work on their behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your minor dependent's investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.

dentalcenter
of northwest ohio

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

Dental Center of Northwest Ohio (the "Dental Center") writes to make you aware of a recent incident that may affect the privacy of some of your personal information. While there is currently no evidence that your information has been misused, we are making you aware of the event, the steps we are taking in response, and steps you may take to better protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? On or about September 1, 2018, the Dental Center's IT vendor, Arakyta, made the Dental Center aware of an issue, at Arakyta, potentially impacting certain Dental Center systems. Arakyta later confirmed ransomware had infected Arakyta systems resulting in a disruption to systems storing Dental Center information. The Dental Center immediately launched an investigation into the nature and scope of incident, including working with third-party computer experts to determine what, if any, Dental Center information was impacted by the Arakyta event. Based on the information provided from Arakyta, on November 7, 2018, the Dental Center confirmed that systems containing Dental Center data were potentially accessible to an unknown actor from August 16, 2018 through September 18, 2018. Although the Dental Center has not received reports of actual access to Dental Center data as a result of the Arakyta event, because the Dental Center was unable to rule out the possibility of such access, the Dental Center is notifying individuals whose information was stored on systems potentially impacted by the Arakyta event.

What Information Was Involved? Through the ongoing investigation, the Dental Center determined that the personal information present on systems impacted by the Arakyta event may include your <<ClientDef1>><<ClientDef2>>(name, address, [and insert all applicable data elements]). To date, the Dental Center has not received any reports of actual or attempted misuse of your personal information as a result of the Arakyta event.

What We Are Doing. The Dental Center takes the confidentiality, privacy, and security of information in our care very seriously. Upon learning of the Arakyta event, we immediately commenced an investigation to confirm the nature and scope of the incident as it relates to Dental Center data. We took steps to identify the personal information stored on systems disrupted by the Arakyta event and we are notifying the individuals who are potentially affected. While the Dental Center has security measures in place to protect information in our care, we are taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security. We are also notifying relevant regulators of the Arakyta event.

As an added precaution, the Dental Center is providing you with access to twelve (12) months of identity monitoring services from Kroll at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information*. You can also enroll to receive the free identity monitoring services through Kroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have questions or concerns, please call our dedicated hotline at 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Please know Dental Center takes the privacy and security of the patient information in our care very seriously and we sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Melinda Cree
Executive Director
Dental Center of Northwest Ohio

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Identity Monitoring

While, to date, the investigation found no evidence that data potentially affected by this incident has been misused, in an abundance of caution, we are offering you access to identity monitoring services through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Information on how to enroll in these services may be found below:

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-???-???-????. Additional information describing your services is included with this letter.

Monitor Your Accounts

In addition to enrolling in the complimentary services detailed above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifacx.com/personal/credit-report-services

In order 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 (5) 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For 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 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. We encourage you to 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.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.