



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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

OS, Inc. ("OS") is writing to inform you of a recent incident that may impact the privacy of some of your information. OS is a Wisconsin company that provides some administrative support services to your current or former healthcare provider, Mercy Health System Corporation ("MHSC"). We wanted to provide you with information about the incident, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened?

On or about December 21, 2018, we learned of suspicious activity occurring within one OS employee's email account. We immediately changed the employee's email credentials, notified law enforcement and launched an investigation. We also began working with forensic experts to determine the nature and scope of the suspicious activity. On February 20, 2019, the investigation confirmed that an unauthorized person gained access to the employee's email account from October 15, 2018 through December 21, 2018, utilizing account credentials obtained through a phishing email campaign.

Although the forensic experts were unable to confirm the specific messages or attachments within the email account that may have been subject to unauthorized access or acquisition, out of an abundance of caution, we began conducting a thorough and systematic review of the impacted email account, working to confirm the identities of the individuals whose information may have been accessible to the unauthorized person. On May 21, 2019, we provided MHSC with a list of the patients whose information may have been accessible within the email account.

What Information Was Involved?

The review of the file determined that the following types of information related to you may have been accessible within the impacted employee email account: name, date of birth, date of service, patient identification number, Social Security number in the form of an insurance identification number, and for a limited number of individuals, medical record number. At this time, we have no evidence of any actual or attempted misuse of the information accessible within the email account. No financial account information or health status information was impacted as a result of this incident.

What We Are Doing.

We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to secure the email account and launched an in-depth investigation to determine the nature and scope of the incident. We also promptly notified your healthcare provider of this incident. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing policies and procedures and implemented additional safeguards to further secure the information in our systems. We will continue working to further secure the information in our systems going forward. We are also notifying regulatory authorities, as required.

As an added precaution, we are also offering complimentary access to 24 months of identity monitoring, fraud consultation and identity theft restoration services. If you wish to receive these services activation instructions are below.

What You Can Do.

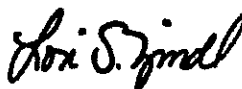
You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*. There you will also find more information on the identity monitoring services we are offering and how to activate them.

For More Information.

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-800-273-7604, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. You may also write to OS at: PO Box 311, Pewaukee, WI 53072.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in black ink that reads "Lori S. Zindl". The signature is written in a cursive, flowing style.

Lori Zindl, President
OS, Inc.

Steps You Can Take to Protect Against Identity Theft and Fraud

To activate Kroll's identity monitoring, fraud consultation, and identity theft restoration services, please follow the steps below:

1. Visit krollbreach.idMonitoringService.com to activate.
2. You have until September 1, 2019 to activate your identity monitoring services. **Your membership number will not work after this date.**
3. Provide your personal information to Kroll, as requested.
4. Provide the following Membership Number: <<Member ID>>.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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 PO 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.equifax.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 19016 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
---	---	--

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.

Although this matter did not involve any credit or debit card information, if you identify any fraudulent or suspicious charges on your credit or debit card, you should immediately contact your bank or financial institution. Incidents of identity theft should also be reported to your local law enforcement.

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.

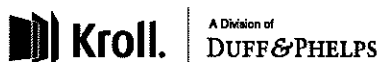
The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with 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 and have a copy of the 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 and your state Attorney General. This notice has not been delayed by law enforcement.

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, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

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, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ 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.