Notice of Data Breach

John Knox Village of Florida ("JKV") is providing notice of a recent data security incident affecting certain personal information of some of its employees and past or present residents. This notice provides information on the incident and what we are doing in response.

What Happened

We recently discovered there may have been an unauthorized disclosure of some certain personal information because of a compromise to one of our employees' email accounts. As a result of the account compromise, certain emails from the employee account may have been forwarded without our knowledge to an external account not affiliated with JKV. Upon learning of the potential incident, we worked with computer forensics experts to thoroughly investigate. While we could not determine through our investigation the exact date range when this email forwarding occurred, we believe it occurred between the dates of approximately March 17, 2021, and March 7, 2022. We then completed a detailed review of emails in the account and, through that process, discovered on May 12, 2022, that some individuals' personal information may have been impacted.

What Information Was Involved

We currently have no knowledge of any actual or attempted misuse of anyone's information. However, through our detailed review of the employee's account, we have determined that one or more of the potentially compromised emails contained certain personal information for some of our employees and past or present residents. This information included names and/or patient account or record numbers and healthcare information, such as medical condition and history, treatment or procedure information, diagnoses, and payment information. In a very small number of instances, the information also included driver's license numbers, Social Security numbers, or other government ID numbers.

What We Are Doing

We take the protection of information seriously and are taking steps to continue investigating this incident, help mitigate the potential for harm, and prevent this from happening again. We have changed the password and secured the affected account to ensure there is no longer any unauthorized access. We also worked with computer forensics experts to complete an analysis of our email system and ensure there was no access to other information outside the single email account. We also notified law enforcement about this incident and will cooperate with any further investigation by them. In addition, we will continue to work internally and with our IT professionals to review our network and email account policies and procedures to identify any other measures we can implement to further strengthen security and help prevent a future incident from occurring.

What You Can Do

We recommend that affected individuals remain vigilant by reviewing and monitoring their account statements and credit reports. If you find any errors or unauthorized activity, you should contact your financial institutions that may be affected. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. In addition, please refer to the document at the

end of this notice titled "Additional Steps to Help Protect Your Information" for more information on protecting your information from misuse.

Additional Safeguards for Affected Individuals

As an additional safeguard, we have arranged for affected individuals to enroll, **at no cost to them**, in 12 months of the online credit monitoring service of *my*TrueIdentity, provided by TransUnion Interactive, a subsidiary of TransUnion®, which is one of the three nationwide credit reporting companies.

Information about how to enroll in this service is provided in written letters being mailed to affected individuals for whom we have available contact information. If you did not receive a letter and believe you may have been affected by this incident, or if would like to determine if you were affected, please contact our dedicated incident response hotline at 855-640-1307.

For More Information

We are very sorry for any concern or inconvenience caused by this incident. If you have any other questions or concerns that you would like to discuss, or to determine if you were impacted by this incident, please contact us through our dedicated incident response hotline at 855-640-1307.

Additional Steps to Help Protect Your Information

Review personal account statements and credit reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. 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 (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, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-866-766-0008	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report suspected fraud. You may contact law enforcement and have the right to file a police report to report suspected identity fraud of theft. Please note that 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 should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Change Online Account Credentials. If the information involved in this incident included credentials used to access any of your online accounts, such as a username, password, PIN, or answer security question, you should to promptly change your username, password, PIN, security question and answer, or other access credentials and take other appropriate steps to protect all online accounts for which you use the same credentials.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **California Residents:** Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.
- **Iowa Residents:** Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, (515) 281-5164.
- **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, (502) 696-5300.
- **Maryland Residents:** Office of the Attorney General of Maryland**,** Consumer Protection Division

200 St. Paul Place Baltimore, MD 21202**,** www.marylandattorneygeneral.gov, (888) 743-0023.

- **New York Residents:** Office of Attorney General, The Capitol, Albany, NY 12224, 1-800-771-7755 (toll-free), https://ag.ny.gov/; and the Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005, (212) 416-8433, https://ag.ny.gov/internet/resource-center
- **North Carolina Residents:** Office of the Attorney General of North Carolina**,** 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, (919) 716-6400.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, (877) 877-9392.
- **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401) 274-4400.
- **Washington D.C. Residents:** Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202)-727-3400, www.oag.dc.gov
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338).

Know 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. You have certain rights under the FCRA, which you can read about by visiting https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf and https://www.consumer.ftc.gov/articles/0070-credit-and-your-consumer-rights. These rights include: (1) You must be told if information in your file has been used against you; (2) You have the right to know what is in your file (you "file disclosure"); (3) You have the right to ask for a credit score; (4) You have the right to dispute incomplete or inaccurate information; (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (6) Consumer reporting agencies may not report outdated negative information; (7) Access to your file is limited to people with a valid need; (8) You must give your consent for reports to be provided to employers; (8) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (9) You may seek damages from violators; and (10) identity theft victims and active duty military personnel have additional rights. For more information, visit www.ftc.gov/credit. States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.