

April 12, 2023

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Portal

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Preliminary Notification: Data Security Incident Involving Kannact, Inc.

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Kannact, Inc. (“Kannact”), a wellness solution consultants that provides consulting services to plan sponsors and group health plans, headquartered in Albany, Oregon, with respect to a recent data security incident that was first discovered on March 13, 2023 (hereinafter, the “Incident”). Kannact takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

As a business associate, Kannact is working to identify and provide notice to all covered entities whose patient data was impacted. This letter will serve to inform you of the nature of the Incident, and what information may have been compromised.

1. Nature of the Incident

On March 13, 2023, Kannact discovered that an unauthorized user had gained access to its network. Upon discovery of this incident, Kannact promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The investigation is still ongoing, however, Kannact is working to identify all the specific individuals and the type of data that was impacted in order to provide sufficient notice. Kannact has provided substitute notice via its website, attached as Exhibit A, and media notice in the form of a press release, attached as Exhibit B. Kannact has not received any reports of fraudulent misuse of the information.

2. Nature of Personal Information

The types of information involved varied by individual. The investigation is still on going, however, the preliminary investigation revealed that the information potentially exposed during

the unauthorized access may have included an individual's name, date of birth, address, phone number, Social Security Number, driver's license number, and protected health information, including, but not limited to, medical diagnosis, treatment, pharmaceutical records, and Kannact ID. **Not all individuals had their social security numbers and or driver's license number impacted.**

As of this writing, Kannact has not received any reports of related identity theft since the date of the Incident (March 13, 2023 to present).

3. Number of Maine residents affected

We believe Maine residents were impacted by this incident, however, Kannact will need to complete data mining to determine the number of individuals and the type of data for each individual. Kannact will provide a supplemental notice to the Office of the Attorney General once a final number is determined and will provide a copy of the notice letter that will be mailed via certified mail to all potentially impacted individuals. The supplemental notice will also identify the covered entities whom Kannact completed notice obligations for.

4. Contact Information

Kannact, Inc. remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact Karen Bridges at my office at Karen.Bridges@WilsonElser.com or 312-706-3023.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

EXHIBIT A

Kannact Inc. Notifies Members of Data Security Incident

[www.Kannact.com on April 12, 2023] Kannact Inc. (“Kannact”) has become aware of a data security Incident that may have resulted in an unauthorized access to some of our members’ sensitive personal information. While we have not received any report of fraudulent misuse of the information, Kannact sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

What Happened? On March 13, 2023, Kannact discovered that an unauthorized user had gained access to its network. Upon discovery of this Incident, Kannact promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. The investigation is still ongoing, however, out of full transparency, Kannact is providing notice about the potential for acquisition of sensitive information by an unauthorized actor. Kannact has not received any reports of fraudulent misuse of the information. Kannact is working to identify all the specific individuals and the type of data that was impacted in order to provide sufficient notice to individuals.

What Information Was Involved? The types of information involved varied by individual. The investigation is still on going, however, the preliminary investigation revealed that the information potentially exposed during the unauthorized access may have included an individual’s name, date of birth, address, phone number, Social Security Number, driver's license number, and protected health information, including, but not limited to, medical diagnosis, treatment, pharmaceutical records, and Kannact ID. **Not all individuals had their social security numbers and or driver’s license number impacted.**

What We Are Doing. Kannact is committed to ensuring the privacy and security of all personal information in our care. Since the discovery of the Incident, Kannact has taken and will continue to take steps to mitigate the risk of future issues. Specifically, Kannact engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Kannact also disabled access to a third party managed file transfer software, deactivated all related API keys, and is improving our patient data ingestion process.

Kannact will be offering complimentary credit monitoring and identity theft protection services to individuals whose social security and driver’s license number was impacted. Notification letters will be sent to those impacted individuals with the information to enroll in the credit monitoring services. Kannact strongly encourages all identified individuals to register for this free service.

What You Can Do. Kannact encourages all members to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that individuals contact his/her financial institution and all major credit bureaus to inform them of such a breach and take the recommended steps to protect his/her interests, including the possible placement of a fraud alert on the credit file. For more information, please see the *Additional Important Information* below.

For More Information. Kannact recognizes that our members may have questions not addressed in this notice. For more information, please call (888) 566-0890 (toll free) between the hours of 8:00 am to 8:00 pm Central Time, Monday through Friday (excluding U.S. national holidays).

Sincerely,
Kannact Inc.

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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

Equifax
P.O. Box 105069
Atlanta, GA 30348
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/>

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. As of September 21, 2018, 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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
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.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your 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 residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 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.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

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).

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - 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.

New York Office of Attorney General - 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>

North Carolina Office of the Attorney General - 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/>.

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov.

EXHIBIT B

Kannact Inc. Notifies Members of Data Security Incident

[Wall Street Journal on April 12, 2023] - Kannact Inc. (“Kannact”) has become aware of a data security incident that may have resulted in unauthorized access to some of our members’ sensitive personal information. While we have not received any report of fraudulent misuse of the information, Kannact sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

On March 13, 2023, Kannact discovered that an unauthorized user had gained access to its network. Upon discovery of this incident, Kannact promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The investigation is still ongoing, however, out of full transparency, Kannact is providing notice about the potential for acquisition of sensitive information by an unauthorized actor. Kannact has not received any reports of fraudulent misuse of the information. Kannact is working to identify all the specific individuals and the type of data that was impacted in order to provide sufficient notice to individuals.

The types of information involved varied by individual. The investigation is still on going, however, the preliminary investigation revealed that the information potentially exposed during the unauthorized access may have included an individual’s name, date of birth, address, phone number, Social Security Number, driver's license number, and protected health information, including, but not limited to, medical diagnosis, treatment, pharmaceutical records, and Kannact ID. **Not all individuals had their social security numbers and or driver’s license number impacted.**

Kannact is committed to ensuring the privacy and security of all personal information in our care. Since the discovery of the incident, Kannact has taken and will continue to take steps to mitigate the risk of future issues. Specifically, Kannact engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. Kannact also disabled access to a third party managed file transfer software, deactivated all related API keys, and is improving our patient data ingestion process.

Kannact will be offering complimentary credit monitoring and identity theft protection services to individuals whose social security and driver’s license number impacted. Notification letters will be sent to those impacted individuals with the information to enroll in the credit monitoring services. Kannact strongly encourages all identified individuals to register for this free service.

Kannact encourages all members to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that individuals contact his/her financial institution and all major credit bureaus to inform them of such a breach and take the recommended steps to protect his/her interests, including the possible placement of a fraud alert on the credit file.

Kannact recognizes that our members may have questions not addressed in this notice. For more information, please call (888) 566-0890 (toll free) between the hours of 8:00 am to 8:00 pm Central Time, Monday through Friday (excluding U.S. national holidays).

Kannact sincerely apologizes for any inconvenience this incident may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,
Kannact Inc.

Kannact Inc. Notifies Members of Data Security Incident

[USA Today on April 12, 2023] - Kannact Inc. (“Kannact”) has become aware of a data security incident that may have resulted in unauthorized access to some of our members’ sensitive personal information. While we have not received any report of fraudulent misuse of the information, Kannact sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

On March 13, 2023, Kannact discovered that an unauthorized user had gained access to its network. Upon discovery of this incident, Kannact promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The investigation is still ongoing, however, out of full transparency, Kannact is providing notice about the potential for acquisition of sensitive information by an unauthorized actor. Kannact has not received any reports of fraudulent misuse of the information. Kannact is working to identify all the specific individuals and the type of data that was impacted in order to provide sufficient notice to individuals.

The types of information involved varied by individual. The investigation is still on going, however, the preliminary investigation revealed that the information potentially exposed during the unauthorized access may have included an individual’s name, date of birth, address, phone number, Social Security Number, driver's license number, and protected health information, including, but not limited to, medical diagnosis, treatment, pharmaceutical records, and Kannact ID. **Not all individuals had their social security numbers and or driver’s license number impacted.**

Kannact is committed to ensuring the privacy and security of all personal information in our care. Since the discovery of the incident, Kannact has taken and will continue to take steps to mitigate the risk of future issues. Specifically, Kannact engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. Kannact also disabled access to a third party managed file transfer software, deactivated all related API keys, and is improving our patient data ingestion process.

Kannact will be offering complimentary credit monitoring and identity theft protection services to individuals whose social security and driver’s license number impacted. Notification letters will be sent to those impacted individuals with the information to enroll in the credit monitoring services. Kannact strongly encourages all identified individuals to register for this free service.

Kannact encourages all members to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that individuals contact his/her financial institution and all major credit bureaus to inform them of such a breach and take the recommended steps to protect his/her interests, including the possible placement of a fraud alert on the credit file.

Kannact recognizes that our members may have questions not addressed in this notice. For more information, please call (888) 566-0890 (toll free) between the hours of 8:00 am to 8:00 pm Central Time, Monday through Friday (excluding U.S. national holidays).

Kannact sincerely apologizes for any inconvenience this incident may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,
Kannact Inc.