WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

July 14, 2021

Anjali C. Das
(312)-821-6164 (direct)
Anjali.Das@WilsonElser.com

Via Online

Attorney General Lawrence Wasden
Office of the Attorney General
700 W. Jefferson Street, Suite 210
P.O. Box 83720
Boise, Idaho 83720-0010

Re: Data Incident Occurred on Kelly Klee, Inc.'s Third Party Vendor, Vertafore
WEMED File No.: 15991.01030

Dear Attorney General:

Our law firm represents Kelly Klee, Inc. ("Kelly Klee"), an insurance broker based in Colorado, in connection with a cybersecurity incident that occurred with Kelly Klee's management software vendor, Vertafore. The incident impacted an insurance management software application called QQ Catalyst. Only on May 28, 2021, Vertafore sent a letter to Kelly Klee of an incident that occurred on November 30, 2020 (the "Vertafore Incident").

A. What Happened: the Vertafore Incident

On or about May 28, 2021, Kelly Klee was notified by a third party software management company, Vertafore, that there was a configuration error in one of Vertafore's insurance agency management applications used by Kelly Klee, which is called QQ Catalyst. According to Vertafore, the configuration error occurred when the QQ Catalyst application was developed by QQ Solutions in 2012, prior to Vertafore's acquisition of the product line. In particular, the QQ Catalyst application was set up with a public configuration, instead of a private configuration. On May 28, 2021, Vertafore informed Kelly Klee via letter that an unauthorized party accessed the publicly available data on or about November 30, 2020. The data did not necessarily pertain to Kelly Klee, but it might have contained information stored by Kelly Klee on QQ Catalyst.

B. Circumstance and Scope of the Vertafore Incident

With respect to Kelly Klee's potentially impacted data, the Vertafore Incident was limited to reports and forms generated by QQ Catalyst when used by Kelly Klee, according to Vertafore. Some of these reports and forms contained names, addresses, birth dates, and driver's license numbers. Thus far, it appears that no other data was input by Kelly Klee in other QQ Catalyst non-designated fields. Moreover, a second set

of data may pertain to documents uploaded by Kelly Klee under the Contact and Policies tabs within the QQ Catalyst application. At this point, Vertafore informed Kelly Klee that, although the above-referenced data may have been accessed, Vertafore has no evidence of misuse of Kelly Klee's sensitive data. Kelly Klee is further investigating what other information, if any, may have been impacted by the incident.

C. Number of Idaho residents affected

Two (2) Idaho residents were potentially affected by this incident. Incident notification letters will be mailed out on July 8, 2021 via First Class Mail. A sample copy of the Incident notification letter mailed to potentially affected resident(s) is included with this letter at **Exhibit A**.

D. Steps Taken in Response to the Vertafore Incident

In response to the Vertafore Incident, Vertafore informed Kelly Klee that the QQ Catalyst configuration was fixed. Vertafore also engaged a leading security firm to search for evidence indicating potential misuse of the information in connection with this event. Vertafore informed Kelly Klee that the firm did not find any evidence of misuse. Furthermore, Vertafore offered to notify the potentially impacted population at no cost for Kelly Klee through Kroll, a third party vendor hired by Vertafore.

At this time, Kelly Klee has no reason to believe that any individual's information has been misused. Out of an abundance of caution, Kelly Klee opted-in so as to avail itself of the notification services offered by Vertafore with respect to individual notification, which include a toll-free call center and credit monitoring services. Thus far, Vertafore provided Kelly Klee a list of 724 individuals whose driver's licenses and dates of birth were stored within the QQ Catalyst application. As stated above, these individuals will be notified by Kroll on behalf of Kelly Klee by July 8, 2021. Moreover, Kelly Klee is in process of identifying other clients whose information could have been contained in the second set of data identified by Vertafore, under the QQ Catalyst Contact and Policies tabs. If Kelly Klee identifies additional clients potentially impacted, Kelly Klee will provide these clients' information to Kroll by July 28, 2021, so as to enable Kroll to notify the individuals by August 9, 2021.

Kelly Klee promptly hired our firm to determine whether Kelly Klee has any other obligations arising from the Vertafore Incident. To this extent, Kelly Klee is notifying you of the Vertafore Incident, as well as applicable attorney generals and regulators. As the Vertafore Incident did not occur Kelly Klee's environment, no forensic investigation was conducted by Kelly Klee. Similarly, Kelly Klee did not notify law enforcement.

E. Contact Information

Kelly Klee remains dedicated to protecting the sensitive information in its control, notwithstanding this incident occurred on its management software application provided by a third party, Vertafore. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very Truly Yours,

Wilson Elser Moskowitz Edelman and Dicker LLP

Anjali C. Das

Anjali C. Das

EXHIBIT A

Vertafore

Important Legal Notice

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<last_name>>,

<<b2b_text_1(AgencyName)>> uses an agency management software and service called QQCatalyst, which is provided by Vertafore. Vertafore takes seriously the responsibility to protect your personal information. As such, we are writing to inform you about a configuration error at Vertafore impacting some of your personal information.

What Happened?

On November 30, 2020, Vertafore discovered a configuration error in its insurance agency management product, QQCatalyst. As a result, there was unauthorized access to reports and forms generated using QQCatalyst. Other files uploaded to QQCatalyst, including insurance applications and quotes, were accessible to the public, though we cannot determine whether these files were actually accessed by unauthorized parties.

Immediately upon becoming aware of the issue, Vertafore fixed the configuration error and secured the potentially affected files. Vertafore has also been investigating the extent to which data may have been impacted and identifying customers and individuals for notification. These investigations take time, and while we have been moving quickly, we have taken time to be sure we're providing accurate information. Vertafore has reported the matter to U.S. federal law enforcement.

What Information Was Involved?

The information impacted could include the following kinds of information: names, addresses, birth dates, and driver's license numbers. In some cases, Social Security numbers, credit card numbers, and bank account information may have been impacted if <<b2b_text_1(AgencyName)>> stored that information in QQCatalyst.

What We Are Doing.

Vertafore engaged a leading security firm to search for evidence indicating potential misuse of the information in connection with this event and did not identify any.

Out of an abundance of caution, Vertafore is offering you one year of free credit and identity monitoring services in recognition that these services offer valuable protection in other contexts beyond this event. More information about these services, including how to activate them, is attached to this notice.

While we continually monitor our network and systems for unusual activity, Vertafore, like any other company, is not immune from this type of event. We maintain information security policies, procedures, practices, and controls, and we are working to further enhance our security tools, policies, and procedures, as well as our security governance and staffing.

What You Can Do.

In addition to taking advantage of the free credit and identity monitoring service, it is always a good idea to remain vigilant against threats of identity theft or fraud. You can do this by regularly reviewing and monitoring your account statements and credit history for any signs of unauthorized transactions or activity. If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police.

It is also always a good idea to be alert for "phishing" emails or phone calls by someone who acts like they know you or are a company that you may do business with and requests sensitive information over email, such as passwords, Social Security numbers, or financial account information.

More information about protecting against identity theft is attached to this notice.

For More Information.

We have set up a call center with additional information about this event, our response, and these services. The call center can be reached by calling 1-855-537-2082 between the hours of 8 a.m. - 5:30 p.m. CT Monday through Friday. We sincerely regret any inconvenience this may cause.

Sincerely,

Vertafore Privacy Team

HOW TO ACTIVATE FREE IDENTITY MONITORING

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. 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.

Visit https://enroll.idheadquarters.com to activate and take advantage of your identity monitoring services.

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

Membership Number: <<Member ID>>

You have been provided with access to the following services 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 will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
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.

ADDITIONAL INFORMATION

To protect against possible fraud, identity theft or other financial loss, you should always remain vigilant, review your account statements and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft, you can contact your local law enforcement agency, your state's attorney general, or the Federal Trade Commission. Please know that contacting us will not expedite any remediation of suspicious activity.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free at +1 (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You may contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax: Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374 +1 (800) 525-6285 www.equifax.com	Experian: Credit Fraud Center P.O. Box 9554 Allen, TX 75013 +1 (888) 397-3742 www.experian.com	TransUnion: TransUnion LLC P.O. Box 2000 Chester, PA 19016-2000 +1 (800) 680-7289 www.transunion.com

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, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

California Residents: Visit the California Office of Privacy Protection (https://oag.ca.gov/privacy) for additional information on protection against identity theft.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov.

Kentucky Residents: The Attorney General can be contacted at Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: +1 (502) 696-5300.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the 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.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9332 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400; or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.