22040

Vertafore

Important Legal Notice

1 1 80 **********AUTO**MIXED AADC 300

[redacted]

May 28, 2021

RE: Notice of Data Event

Dear Valued QQCatalyst Customer,

I am reaching out to you personally to let you know about a data event potentially impacting the personal information of your customers. If you are a current QQCatalyst customer, you may have received or will be receiving, an alert about this event in QQCatalyst.

On November 30, 2020, Vertafore discovered a configuration error in its insurance agency management product, QQCatalyst. The configuration error occurred when the application was developed by QQSolutions in 2012, prior to Vertafore's acquisition of the product line. Vertafore's other products and services are not impacted.

The configuration error resulted in the unauthorized access to reports and forms generated by QQCatalyst users in your company. Some of these reports and forms contain names, addresses, birth dates, and driver's license numbers. While our systems are not intended to keep Social Security numbers or payment information, if you stored this information in reports and forms, it also was impacted. Any other files uploaded by QQCatalyst users to the Contact and Policies tab, including insurance applications and supporting documentation, were also accessible to the public, though we cannot determine whether these files were actually accessed by unauthorized parties. This event was limited to your customers' information, and we have no evidence that other information related to your agency was impacted.

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

You may need to notify individuals and regulators of this event. Vertafore is making available to you no-cost services and resources to help you notify and support your customers, including free credit and identity monitoring services. These services will be provided by Kroll.

To learn more about the event, the impacted data, what you may need to do, and the no-cost services and resources available, please visit redeem.cyberdetecter.com and create an account. When you access the website, **you will be required to enter this code –** [redacted] **– to set up your account.**

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.

We recognize and value the trust you place in us and our solutions, and we are committed to continuing to earn that trust.

Sincerely,

Amy Zupon
CEO, Vertafore

MORE INFORMATION

As noted in the enclosed letter, because of the QQCatalyst event, you may have a legal duty to notify certain of your customers, state attorneys' general or other regulators. If you are a current QQCatalyst customer, you may have received or will be receiving, an alert about this event in QQCatalyst.

To learn more about the event, the impacted data, what you may need to do, and the no-cost services and resources available, please visit the CyberDetectER Portal ("Portal") redeem.cyberdetecter.com and create an account. When you access the Portal, **you will be required to enter this code – [redacted] – to set up your account.**

You have until June 28, 2021 to take advantage of these services.

Additional information is included below.

What Happened?

On November 30, 2020, Vertafore discovered a configuration error in its insurance agency management product, QQCatalyst. The configuration error occurred during development of the QQCatalyst application, prior to when Vertafore acquired the product line. As a result, there was unauthorized access to reports and forms generated by QQCatalyst users and linked to in an online forum. Other files uploaded by QQCatalyst users, including insurance applications and quotes, were also accessible to the public, though Vertafore cannot determine whether these files were actually accessed by unauthorized parties. Vertafore's other products and services are not impacted. This event was limited to your customers' information, and we have no evidence that other information related to your agency was impacted.

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

What Data Was Impacted?

The configuration error existed between 2012 and December 2020 and resulted in two categories of files being stored in locations that were publicly accessible.

First, reports and forms that you generated within QQCatalyst were publicly accessible. A security researcher accessed some of these files and alerted us to the issue. We do not have evidence to determine whether others accessed these files without authorization, some of which contain names, addresses, birthdates, and driver's license numbers. We have searched for and extracted names and contact information for these individuals and are making them available to you in the Portal. While our systems are not meant to store Social Security numbers or payment information, if you stored this information in QQCatalyst in reports and forms, it also was also impacted.

Second, any file that is in the Contact and Policies tab on QQCatalyst was also publicly accessible due to the configuration error, though we cannot determine whether these files were actually accessed by unauthorized parties. Accordingly, if you uploaded files to the Contact and Policies Files tab containing personal information about individuals, you may add those individuals to be notified at no cost to you.

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

What You Need to Do:

You may need to notify individuals and regulators about the event because you are the owner of the impacted data. Specifically, you may need to notify:

1. **Individuals.** All 50 states have laws requiring notification to state residents following certain specified security events involving personal information. The kinds of personal information and security events covered by these laws vary by state.
2. **State Attorneys General or Other Agency.** Many state laws also require notification to the state Attorney General or another agency when a state resident has personal information impacted in a security event.

3. **State Insurance Commissioners.** Certain state laws also require registered entities or certain other specified entities to notify the state Insurance Commissioner.

It is your decision regarding whether to notify any individuals or regulators. This summary does not constitute legal advice, and you may want to consult with your own legal counsel regarding these issues.

What We're Doing to Support You:

Vertafore is making available to you no-cost services and resources to help you notify and support your customers, including free credit and identity monitoring services. These services will be provided by Kroll.

To access the available no-cost services and resources available, please visit the Portal redeem.cyberdetecter.com and create an account. When you access the Portal, **you will be required to enter this code – [redacted] – to set up your account.**

Vertafore has undertaken the following actions to support you:

- **Data Identification:**
  - We undertook a process designed to extract impacted data from reports, forms, and other files generated through normal operations of the QQCatalyst solution that we identified as containing personal information and then individuals to whom that information may belong.
  - We did not review files that you uploaded to QQCatalyst, and we did not extract information that QQCatalyst is not designed to maintain such as Social Security numbers and financial information.
- **Notification Support:** We have partnered with Kroll and their CyberDetectER service to provide you with a set of tools to support your efforts to notify impacted customers. In the Portal, you can:
  - View the names of the individuals whose personal information we identified
  - Choose whether you would like us to send individual notifications on your behalf
  - Choose which individuals you would like us to notify
  - Review content of individual notices
  - Receive confirmation after individuals have been notified
  - Find and download information you can use to notify state Attorneys General, Insurance Commissioners or other regulators.
- **Credit Monitoring and Support:** We are offering free credit monitoring to any of your customers to whom you want to offer it, as well as any of your customers that contacts us directly.

What Happens Next:

To access the available no-cost services and resources available, please visit redeem.cyberdetecter.com and create an account. When you access the Portal, **you will be required to enter this code – [redacted] – to set up your account.**

After you create an account, you will have access to the variety of notification support services and tools described above, as well as instructions on how to use them.

IMPORTANT: You have until June 28, 2021 to take advantage of our notification support services, make your elections, and provide contact information for individuals you want to be notified.

Questions and Additional Information

Your best source of information is the Portal. It contains additional information about the event, responses to frequently asked questions, and a step-by-step guide for leveraging our notification support services. If you have questions about accessing the Portal or leveraging the available services, please contact 1-855-608-3456.

You may also email questions@vertafore.com or your customer support representative if you have other questions.

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

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.

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.