Classical Conversations
Classical Christian Community

255 Air Tool Drive
Southern Pines, NC 28387
CLASSICALCONVERSATIONS.COM

<<Recipient FirstName>> <<Recipient LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

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

Notice of Data Breach

Dear <<Recipient FirstName>>,

Classical Conversations, Inc. ("CC") values the privacy of our employees and contractors. We are writing to notify you about a data security incident we recently experienced, which may have impacted your personal information. In this letter, we explain what happened, the steps we have taken to address the situation, and how we are providing you support in light of the security incident. We have also outlined additional steps you may take to protect yourself against potential misuse of your personal information.

What Happened

On Tuesday, June 6, 2023, we were first contacted by a contractor, who informed us that she was able to view the personal information of other employees and contractors when using our third party HR software. Shortly thereafter, we heard from additional contractors regarding the same issue with the HR software. That software is designed to allow employees and contractors to review only their own personal information. Upon learning of the issue, we immediately began investigating and contacted the HR software service provider to determine the cause and how to resolve it. We learned that the incident resulted from an unintentional misconfiguration of the HR software system done at the direction of the software service provider. This misconfiguration allowed certain current and former contractors to view the personal information of current and former employees and contractors between March 14, 2023, and June 7, 2023. We reconfigured the HR system by the next day, June 7, 2023. It is now functioning properly, and employees and contractors can only see their own personal information.

What Information Was Involved

The personal information that may have been impacted by this incident included: first, middle, and last name; maiden name; address; Social Security number; date of birth, marital status; gender; disability; ethnicity/race; veteran status; home and work email; telephone number; LinkedIn profile URL; emergency contacts; and direct deposit (including bank name, routing number, account number) information.

Here's What We Are Doing

We have consulted with cybersecurity experts and have worked with our HR software service provider to respond to and investigate this incident. We have reconfigured the HR software system so that each employee's or contractor's data is only available to that employee or contractor.

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 24-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 **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

Classical Christian Community

255 Air Tool Drive
Southern Pines, NC 28387
CLASSICALCONVERSATIONS.COM

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

Membership Number: **<<Member ID>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do

Please review the enclosed "*Additional Information on Credit Monitoring & Identity Theft*" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. It is recommended that you remain vigilant for incidents of fraud and identity theft and report suspected incidents of identity theft to local law enforcement or the attorney general. We recommend that you carefully monitor your free credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. You should also regularly review your credit or debit card account statements to determine if there are any discrepancies or unusual activity listed. If you see something you do not recognize, immediately notify your financial institution.

For More Information

If you have any further questions or concerns regarding this matter, please contact 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Rex E. Elliott, CFO/COO

ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements, monitoring free credit reports, and promptly reporting any fraudulent activity or suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

- You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), https://consumer.ftc.gov/features/identity-theft
- You have certain rights under the **Fair Credit Reporting Act** related to your consumer credit. For more information, please see https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Take Charge: Fighting Back Against Identity Theft: This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action. You also can contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For District of Columbia residents: You may contact the District of Columbia Attorney General, 400 6th Street, NW, Washington, D.C. 20001, oag@dc.gov, 202-727-3400.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Rhode Island residents: You may contact the Rhode Island Attorney General, 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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.