



Kamran Salour
650 Town Center Drive, Suite 1400
Costa Mesa, CA 92626
kamran.salour@lewisbrisbois.com
Direct: 714.966.3184

November 14, 2023

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Email: idtheft@oag.state.md.us

Re: Notification of Data Security Incident

To Whom It May Concern:

Lewis Brisbois represents Emmanuel University, a private college located in Franklin Springs, Georgia, in conjunction with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland data breach notification law.

1. Nature of the Security Incident

On or around October 17, 2023, Emmanuel University learned that a spreadsheet containing student information was inadvertently disseminated via email to a limited amount of Emmanuel University students and their parents. Emmanuel University immediately attempted to recall the email. In the instances where it was unable to do so, Emmanuel University emailed the students and parents informing them of the inadvertent disclosure and requested that they delete the email and information contained therein.

2. Type of Information and Number of Maryland Residents Affected

Emmanuel University notified three (3) Maryland residents of this data security incident via first class U.S. mail on November 14, 2023. The information accessed by the recipients of the spreadsheet may have included name and Social Security number information. A sample copy of the notification letter sent to these individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

Emmanuel University has implemented additional protocols and trainings in an effort to prevent a similar incident from occurring in the future. Further, Emmanuel University has offered all individuals whose information was involved twelve (12) months of complimentary services through Kroll, which includes credit monitoring, fraud consultation services, identity theft restoration services, and access to a call center.

4. Contact Information

Emmanuel University remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (714) 966-3184 or by email at Kamran.Salour@lewisbrisbois.com.

Regards,

A handwritten signature in black ink, appearing to read "Kam Salour", with a stylized flourish at the end.

Kamran Salour of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enc.: Sample Consumer Notification Letter



Emmanuel University
181 Spring Street
Franklin Springs, Georgia 30639

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

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

<<b2b_text_1 (Subject Line)>>

Dear <<first_name>> <<last_name>>:

Emmanuel University is writing to notify you of a recent data security incident that involved your personal information. Emmanuel University takes the privacy and security of your personal information very seriously. As a result, Emmanuel University is informing you of this incident, the steps you can take to help protect your personal information and offering you complimentary identity monitoring services.

What Happened? On or around October 17, 2023, Emmanuel University learned that a spreadsheet containing student information was inadvertently disseminated via email to a limited amount of Emmanuel University students and their parents. Emmanuel University immediately attempted to recall the email. In the instances where it was unable to do so, Emmanuel University emailed the students and parents informing them of the inadvertent disclosure and requested that they delete the email and information contained therein.

What Information Was Involved? The impacted information may have included your name and Social Security number.

What Are We Doing? As soon as Emmanuel University discovered the incident, it took the steps described above. Emmanuel University also implemented additional protocols and trainings to minimize the risk of a similar incident occurring in the future. Emmanuel University is further notifying you of this event and advising you about steps you can take to help protect your personal information.

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.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number (S_N)>>

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 Can You Do? Emmanuel University recommends that you review the guidance included with this letter about how to protect your personal information. In addition, Emmanuel University recommends activating the complimentary services being offered through Kroll to further help protect your personal information. To receive identity monitoring services, you must be over the age of eighteen (18) and have established credit in the U.S., have a Social Security number to your name, and have a U.S. residential address associated with your credit file.

For More Information. If you have any questions regarding the incident, please call <TFN> between 8:00 A.M. CST to 5:30 P.M. CST, Monday through Friday, excluding holidays.

Emmanuel University appreciates your understanding and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Emmanuel University

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

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 <http://www.annualcreditreport.com/>, calling toll-free 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



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.