



STATE OF NH  
DEPT OF JUSTICE

2021 MAR 25 PM 1:04

Squire Patton Boggs (US) LLP  
4900 Key Tower  
127 Public Square  
Cleveland, Ohio 44114

O +1 216 479 8500  
F +1 216 479 8780  
squirepattonboggs.com

Colin R. Jennings  
T +1 216 479 8420  
colin.jennings@squirepb.com

March 22, 2021

**SENT VIA U.S. MAIL**

Office of the Attorney General  
State of New Hampshire  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of a Security Breach**

To Whom It May Concern,

This letter shall serve as notice to the New Hampshire Attorney General on behalf of our client, Kentucky Wesleyan College (“KWC”), of a security breach that involved the personally identifiable information (“PII”) of approximately five (5) New Hampshire residents.

On or about September 22, 2020, KWC experienced a security breach, which resulted in the compromise of certain servers maintained by KWC. KWC became aware of such security breach on or about September 22, 2020. In response, among other things, KWC immediately retained an IT firm to conduct a thorough forensic investigation into the circumstances surrounding the incident.

Based upon its investigation, KWC learned that this incident may have resulted in the unauthorized access to the PII of approximately five (5) New Hampshire residents. The types of PII that may have been accessed include the Social Security Number.

The affected New Hampshire residents will be sent written notification of the incident in the form attached herewith on or about March 22, 2021. A template notification is attached herewith, with the types of affected PI redacted, for your office to use in connection with any public disclosure of the incident.

45 Offices in 20 Countries

Squire Patton Boggs (US) LLP is part of the international legal practice Squire Patton Boggs, which operates worldwide through a number of separate legal entities.

Please visit [squirepattonboggs.com](http://squirepattonboggs.com) for more information.

Squire Patton Boggs (US) LLP

Office of the Attorney General

March 22, 2021

**SENT VIA U.S. MAIL**

KWC takes very seriously its responsibility to protect the privacy of the personal information of New Hampshire residents. Any questions about this incident can be directed to me at [colin.jennings@squirepb.com](mailto:colin.jennings@squirepb.com).

Sincerely,

Squire Patton Boggs (US) LLP



Colin R. Jennings

cc: Dan Frazier, Vice President of Finance

Encl: Template Adult Individual Notification Letter

SENT VIA U.S. MAIL

Kentucky Wesleyan College  
<Return Name>  
<Return Address>  
<City> <State> <Zip>



<FirstName> <LastName>  
<Address1>  
<Address2>  
<City><State><Zip>

<<Date>>

Dear <<First Name>>:

We are writing to share with you important information regarding a network security incident that potentially involved your personally identifiable information (“PII”). We take this incident very seriously and are providing you with information, as well as access to resources, so that you can better protect your PII.

**What Happened:**

On or about September 22, 2020, Kentucky Wesleyan College (“KWC”) experienced a network security incident, which resulted in the compromise of certain servers maintained by KWC. After a thorough investigation, KWC learned that this incident may have resulted in the compromise of PII of certain members of the KWC community. While we have no information to suggest that your information was misused, we wanted to provide this notification to you out of an abundance of caution, so that you may diligently monitor your accounts.

**What Information Was Involved:**

The PII that could have been accessed by the unauthorized individual may have included your: <<Type of Information Identified>>.

**What KWC is Doing:**

The confidentiality of PII is one of KWC’s top priorities. Immediately upon learning of the incident, we took steps to ensure that the unauthorized individual no longer had access to our system and took steps to investigate and contain the incident. We retained a third party IT firm to conduct a thorough forensic investigation and to assist in the remediation of our system, to include implementing additional security measures. As such, we have already strengthened our system, and will continue to do so throughout this response process and beyond.

SENT VIA U.S. MAIL

**Credit Monitoring Services:**

While KWC is not aware of any identity fraud or improper use of any PII as a direct result of this incident, out of an abundance of caution, we have arranged to have Cyberscout provide you with twenty-four (24) months of complimentary credit monitoring services and identity theft insurance. To activate your membership in these services, please follow the steps outlined at the end of this letter.

**What You Can Do:**

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please contact your financial institution. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

**For More Information:**

If you have any questions about this notice or the incident, please visit our website at <https://kwc.edu/> or telephone the Cyberscout call center at 1-866-752-0071 from 8:00 am to 8:00 pm CT, Monday through Friday, for ninety (90) days from the date of this letter.

We value you and sincerely apologize for any inconvenience caused by this incident. Thank you for your understanding.

Sincerely,



Dr. Thomas Mitzel,  
President, Kentucky Wesleyan College

SENT VIA U.S. MAIL

### **Cyberscout Credit Monitoring Services**

In response to the network security incident, KWC has engaged Cyberscout to provide the following services:

- **Single Bureau Credit Monitoring\***;
- **Identity Theft Insurance.**

These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. A notification will be sent to you the same day that the changes or updates takes place with the bureau. Further, in the event that you become a victim of fraud or of identity theft, Cyberscout will provide you with a \$1,000,000 insurance reimbursement policy. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated.

Cyberscout representatives are available for ninety (90) days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm CT, Monday through Friday. Please call the Cyberscout help line 1-866-752-0071 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

#### **How do I enroll for the free services?**

To Register your account and activate your services:

1. Type the following URL into your browser: <https://www.cs2protect.com> or **cs2protect.com**
2. Click the "Sign Up" button and follow the instructions to create your account.
3. Enter your information and the following Access Code to complete your registration:  
<<Access Code>>
4. Next, click the "Use Now" link on the Monitoring Services file to verify your identity and activate your monitoring services.

Important – you must register your account and activate your monitoring services within 90 days from the date of this letter, otherwise your ability to access the services will expire.

\* Services marked with an "\*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

SENT VIA U.S. MAIL

Additional Information

To protect against possible fraud, identity theft or financial loss, we encourage you to 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 reporting agencies and additional information about steps you can take to obtain a free credit report and to place a fraud alert, credit freeze, or credit lock on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your State's Attorney General, or the Federal Trade Commission.

## INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one (1) free credit report annually from each of the three (3) major credit reporting agencies. To order a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free (877) 322-8228.

## INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three (3) credit reporting agencies below:

Equifax:  
Consumer Fraud Div.  
P.O. Box 740256  
Atlanta, GA 30374  
1-888-766-0008  
[www.equifax.com](http://www.equifax.com)

Experian:  
Credit Fraud Center  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion:  
TransUnion LLC  
P.O. Box 2000  
Chester, PA 19022-  
2000  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)

**Fraud Alert:** Consider contacting the three (3) major credit reporting agencies 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.

To place a fraud alert, contact any of the three (3) major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts ninety (90) days, but can be renewed.

**Credit Freeze:** A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. There is no cost to place a credit freeze. When a credit freeze is in place, no one—including you—can open a new account. As a result, 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.

**SENT VIA U.S. MAIL**

To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

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 the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven (7) years.

**Credit Lock:** Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three (3) credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

#### ADDITIONAL RESOURCES

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, 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](http://www.consumer.gov/idtheft).

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.

SENT VIA U.S. MAIL

**Maryland Residents:** The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or <http://www.oag.state.md.us>.

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

**Iowa Residents:** The Attorney General can be contacted at 1305 E. Walnut St. Des Moines, IA 50319; (515) 281-5164; or <https://www.iowaattorneygeneral.gov/>.

**Oregon Residents:** The Attorney General can be contacted at 1162 Court St. NE Salem, OR 97301-4096; (877) 877-9392; or <https://www.doj.state.or.us/>.

**Rhode Island Residents:** The Attorney General can be contacted at 4 Howard Avenue Cranston, RI 02920; (401) 274-4400; or <http://www.riag.ri.gov/index.php>. You may also file or obtain any police report filed in regard to this incident.

**District of Columbia Residents:** The Attorney General can be contacted at Office of Attorney General, 400 6th Street, NW, Washington, DC 20001; (202) 727-3400; or <https://oag.dc.gov/>.