

December 2, 2021

**VIA CERTIFIED MAIL – RETURN RECEIPT REQUESTED**

Attorney General John M. Formella  
Office of the Attorney General  
Department of Justice  
33 Capitol Street  
Concord, NH 03301

**RECEIVED**  
**DEC 06 2021**  
**CONSUMER PROTECTION**

RE: Data Incident Notification

Dear Attorney General Formella:

Our firm represents Elizabethtown College (the “College”). The College hereby formally submits notification of a recent data incident pursuant to NH Rev Stat § 359-C:20. The College reserves the right to supplement this notice with any significant details learned subsequent to this submission. By providing this notice, the College does not waive any rights or defenses regarding the applicability of New Hampshire law, including the applicability of NH Rev Stat § 359-C:20, the applicability of any other laws of this or any other state, or the existence of personal jurisdiction over the College.

On November 2, 2021, the College became aware that between February 2019 and November 2021, five files that contained the names, Social Security numbers, and/or addresses of members of the College community were saved in a shared folder accessible to users of the College’s network (the “Incident”). Immediately upon learning of the Incident, the College moved the files to a private folder. By the end of the week, the College retained outside counsel specializing in data security incidents and began investigating. At this time and based upon our investigation, the College does not have any evidence that any individuals’ personal information was accessed or stolen. Nonetheless, out of an abundance of caution, the College has decided to notify your office (via this letter) and the two (2) New Hampshire residents potentially affected by this Incident on or about December 2, 2021. A sample notification letter to affected residents is attached hereto as Exhibit A.

The College takes the security of personal information seriously. It discovered the Incident while routinely reviewing its computer systems to ensure that all information was properly categorized and adequately protected. The College has completed that review, secured the miscategorized data, and continues taking steps to protect the privacy of members of the College’s community. In addition, the College has retained Kroll, Inc. to provide notice to affected individuals and Experian to provide free identity theft and credit monitoring services. Please do not hesitate to contact me if you have any questions regarding this matter.

Attorney General John Formella  
December 2, 2021  
Page 2

Sincerely,

GODFREY & KAHN, S.C.

A handwritten signature in black ink, consisting of a large, stylized loop on the left and a long, horizontal stroke extending to the right.

Justin P. Webb

JPW

**EXHIBIT A**

**Sample Notification Letter**



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

<<first\_name>> <<last\_name>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

## NOTICE OF DATA BREACH

Dear <<first\_name>> <<last\_name>>,

Elizabethtown College ("the College", "we", "us", or "our") recently discovered that five files containing sensitive information were improperly secured and may have contained your personal information. We are writing, as a precautionary measure, to notify you of the incident and provide more details about it because the College values the security and privacy of your personal information, is committed to ensuring you understand what happened, and wants to provide you with the tools to assist you with securing and protecting your personal information if you have ongoing concerns.

### What happened?

On November 2, 2021, the College became aware that between February 2019 and November 2021 five files containing personal information were saved in a shared folder accessible to all users of the College's network, including faculty, staff, and students.

Immediately upon learning of the incident, the College moved the files to a private folder, began investigating, and retained counsel who routinely respond to data security incidents.

At this time and based upon our investigation, the College does not have any evidence that your information, in particular, was accessed or acquired by a third party. The College also has not received any reports of misuse of any personal information contained in the files. We know only that members of the College community *could have* accessed your information. Please also note that the shared folder in which these files were stored was accessible only on the College's network—it was not accessible through the Internet or to third parties without a login and password to the College's systems.

The College is nonetheless providing this notification because we greatly value the security and privacy of individuals in our College community. We take this matter seriously, and we encourage you to take appropriate action, in conjunction with our efforts, to minimize or eliminate potential harm if your personal information was compromised.

### What information was involved?

The personal information that was *potentially* accessible on the College's network consisted of your name, Social Security number, and address.

### What we are doing.

The College values the security and privacy of everyone in our community and deeply regrets that this incident occurred. The College discovered this incident while routinely reviewing its computer systems to ensure that all information was properly categorized and adequately protected. The College has completed that audit, secured the miscategorized data, and continues taking steps to protect the privacy of the College's students and alumni. Where required, we have also reported this incident to the appropriate law enforcement authorities.

As an added precaution to help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. Ensure that you **enroll by:** <<b2b\_text\_6(EnrollmentDeadline)>>. (Your code will not work after this date.) To activate your membership and start monitoring your personal information please follow these two simple steps:

1. Visit the **Experian IdentityWorks website:** <https://www.ExperianIDWorks.com/3bcredit>
2. Provide your **activation code:** <<ActivationCode (S\_N)>>

If you have questions about the IdentityWorks product, need assistance with identity restoration, or would like an alternative to online enrollment in IdentityWorks, please contact Experian's customer care team at 877-288-8057 by <<b2b\_text\_6(EnrollmentDeadline)>>. Be prepared to provide Engagement Number <<b2b\_text\_1(EngagementNumber)>> as proof of eligibility.

A credit card is not required for enrollment in Experian IdentityWorks, and your enrollment grants you access to the following features:

- **Experian credit report at signup:** See what information is associated with your credit file.<sup>1</sup>
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit- and non-credit-related fraud.
- **Experian IdentityWorks ExtendCARE™:** You may elect to continue receiving the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

The Experian IdentityWorks website provides additional information about each of these features, as well as self-help tips and information about identity protection at this site.

#### **What you can do.**

To date, the College has not received any reports of misuse of your data (or any of the data contained in the impacted files). However, if you are concerned about your personal information, please consider:

- enrolling in the Experian IdentityWorks program described above;
- referring to the "Additional Resources" section included with this letter, which includes additional steps you can take to protect your information, recommendations from 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;
- monitoring your financial accounts and promptly contacting your financial institution if you see any evidence of unauthorized activity; and
- promptly reporting any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

#### **For more information.**

Protecting your information is important to us. While we trust that the services we are offering to you demonstrate our continued commitment to your security and privacy, we also sincerely apologize for any inconvenience and concern this incident may cause you.

If you have further questions about this incident or need additional information and assistance, please contact the Elizabethtown College Business Office at (717) 361-1417 between 8:00 a.m. and 4:30 p.m. EST daily or by e-mail at [businessoffice@etown.edu](mailto:businessoffice@etown.edu).

Sincerely,



Elizabeth Rider  
Provost & Senior Vice President for Academic Affairs  
Elizabethtown College

<sup>1</sup>Individuals who enroll online in IdentityWorks can also elect to receive daily credit reports.

<sup>2</sup>Please note that this Identity Restoration support is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration).

## ADDITIONAL RESOURCES

### **Contact information for the three nationwide credit reporting agencies:**

**Equifax**, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

**Experian**, PO Box 2104, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

**TransUnion**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-888-4213

**Free Credit Report.** It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

### **For Colorado, Georgia, Maine, Maryland, Massachusetts, 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.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-IDTHEFT (438-4338).

**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](http://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](http://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 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](http://www.ct.gov/ag).

**For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html)

**For California Residents:** You may also wish to review the information provided by the California Attorney General at <https://oag.ca.gov/idtheft>.

**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 at [consumer@ag.iowa.gov](mailto:consumer@ag.iowa.gov), by calling (515) 281-5926, or writing to 1305 E. Walnut Street Des Moines, Iowa 50319-0106.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at <https://doj.state.or.us>, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.