

# **EXHIBIT 1**

By providing this notice, Baker University does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

### **Nature of the Data Event**

In December 2024, Baker University discovered suspicious activity related to certain systems which resulted in a network outage. Baker University immediately took steps to secure their environment and launched an investigation to determine the nature and scope of the activity. The investigation determined there was unauthorized access and/or acquisition of certain files and folders within Baker University's network between December 2, 2024, and December 19, 2024. As a result, Baker University began an extensive review of these files and folders to determine whether sensitive information may have been impacted and to whom it related. This review was recently completed.

The information that could have been subject to unauthorized access includes name, Social Security number, and financial account information.

### **Notice to Maine Residents**

On or about December 19, 2025, Baker University provided written notice of this incident to five (5) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

### **Other Steps Taken and To Be Taken**

Upon discovering the event, Baker University moved quickly to investigate and respond to the incident, assess the security of Baker University systems, and identify potentially affected individuals. Further, Baker University notified federal law enforcement regarding the event. Baker University is also working to implement additional safeguards and training for its employees. Baker University is providing access to credit monitoring services for one (1) year through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Baker University is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Baker University is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

# **EXHIBIT A**



<<Return Mail Address>>  
<<City>>, <<State>> <<Zip>>

<<Name 1>> <<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXXXX>>  
Enrollment Deadline: March 19, 2026

To Enroll, Scan the QR Code Below:



Or Visit:  
<https://app.idx.us/account-creation/protect>

December 19, 2025

## NOTICE OF <<Variable Data 2>>

Dear <<Name 1>> <<Name 2>>:

Baker University is writing to inform you of an incident that may impact the security of some of your information. While we are unaware of any actual or attempted identity theft or fraud in relation to this incident, we are providing you with information about the incident, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** In December 2024, Baker University discovered suspicious activity related to certain systems which resulted in a network outage. We immediately took steps to secure our environment and launched an investigation to determine the nature and scope of the activity. The investigation determined there was unauthorized access and/or acquisition of certain files and folders within our network between December 2, 2024, and December 19, 2024. As a result, Baker University began an extensive review of these files and folders to determine whether sensitive information may have been impacted and to whom it related.

**What Information Was Involved?** Baker University is notifying you now because the review recently determined that certain information relating to you may have been within the accessed and/or acquired files and folders, including your name and <<Variable Data 3>>.

**What We Are Doing.** We take this incident and the security of information in our care very seriously. Upon becoming aware of this incident, we immediately took steps to confirm the security of our environment. We reviewed existing security policies and implemented additional measures to further protect against similar incidents moving forward. We reported this incident to law enforcement and regulators, as required by law.

As an added precaution, Baker University is offering you complimentary access to <<12/24>> months of credit monitoring through IDX. Details of this offer and instructions on how to enroll in the services may be found in the attached *Steps You Can Take to Help Protect Your Personal Information*. Please note that, due to privacy restrictions, we are unable to automatically enroll you in the offered identity monitoring services.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Personal Information*.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-844-948-2042 Monday through Friday, 9:00 a.m. to 9:00 p.m., Eastern Time. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you. You can also write to Baker University at P.O. Box 65, Baldwin City, KS 66006.

Sincerely,  
Baker University

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

### Enroll in Monitoring Services

**1. Website and Enrollment.** Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is March 19, 2026.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**3. Telephone.** Contact IDX at 1-844-948-2042 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

### Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/data-breach-help">https://www.transunion.com/data-breach-help</a>
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160,  
Woodlyn, PA 19094

## Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

*For District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and [oag.dc.gov](http://oag.dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://oag.maryland.gov>.

*For New Mexico residents*, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<XX>> Rhode Island residents that may be impacted by this event.