

00001
ACD123400001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 11, 2016

Re: Notice of a Data Breach

Dear John Sample:

Kalamazoo College is committed to maintaining the privacy and security of our current and former employees' personal information. We are writing to inform you of an incident involving your personal information and to provide you with information on the steps we are taking to protect you and your information moving forward.

What Happened?

On April 29, 2016, we learned that a targeted "spear phishing" email message had been sent to a Kalamazoo College employee on the afternoon of April 28, 2016. Spear phishing emails are an attempt by an individual or group to solicit personal information from unsuspecting users by posing as someone known to the recipient. The email our employee received was designed to appear as though it had been sent by a Kalamazoo College administrator and requested faculty, staff and student employees' 2015 IRS Form W-2 *Wage and Tax Statements*. Believing the email to be legitimate, the employee replied to the message and attached the 2015 IRS Forms W-2, which included your name, address, Social Security number, and earnings information.

We have notified the IRS, FBI, and the Michigan State Police of the incident. The IRS has indicated to us that they will monitor affected employees' accounts for the purposes of attempting to prevent disbursement of fraudulent tax refunds. We also have informed the state taxing authorities of the incident.

What Information Was Involved?

The information involved in this incident included the names, addresses, Social Security numbers, and earnings for anyone who was a Kalamazoo College employee and was issued an IRS Form W-2 Wage and Tax Statement for the 2015 tax year.

What We Are Doing.

We recognize this issue can be frustrating and we are taking steps to help protect you and to safeguard employee personal information going forward. As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem



arises, simply call 1-855-904-5756 (toll-free) or +1-512-201-2174 (toll) and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use the AllClear PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-904-5756 (toll-free) or +1-512-201-2174 (toll) using the following redemption code: Redemption Code.

If you live outside the United States, you will not be able to enroll online without a U.S. address and phone number. To register for the PRO service, you will need to call 1-855-904-5756 (toll-free) or +1-512-201-2174 (toll) and provide an email address in order to receive alerts associated with your monitoring service.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. The College is aggressively analyzing where policy and process changes are needed, including analysis of additional automated technology solutions, and will take the appropriate actions. We will supplement existing employee training with additional training on protecting personal information.

What You Can Do.

Detailed information about the AllClear ID membership and instructions on how to enroll is included with this letter. In addition to enrolling in the 24 months of AllClear ID services, there are actions you can take to mitigate the chances of fraud or identity theft. Additional information about preventing fraud and identity theft is included with this letter.

For More Information.

Should you have further questions regarding this incident, you may call 1-855-904-5756 (toll-free) or +1-512-201-2174 (toll) Monday through Saturday, 8:00 a.m. to 8:00 p.m., Central Standard Time.

I deeply regret any concern this incident has caused you.

Sincerely,



Eileen B. Wilson-Oyelaran
President

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements

To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
 - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”)
- Incurred by you from an Event that did not occur during your coverage period;



- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the AllClear Secure eligibility database, please contact AllClear ID:

<p><u>E-mail</u> support@allclearid.com</p>	<p><u>Mail</u> AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701</p>	<p><u>Phone</u> 1.855.434.8077</p>
--	---	---

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

Even if you choose not to take advantage of the identity theft protection services we are offering, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every 12 months. To order your credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax

P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
(800) 685-1111

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
(888) 397-3742

TransUnion

P.O. Box 2000
Chester, PA 19016
www.transunion.com
(800) 916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
(877) 438-4338

If you are a resident of Maryland, you may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

If you are a resident of North Carolina, you may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400.

Fraud Alerts: There are also two types of fraud alerts that 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 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with 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 calling the toll-free fraud number of any of the three national credit reporting agencies listed below.



Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.