Florida Keys Community College

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

RE: Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

Florida Keys Community College (the "College") recently discovered that it became the target of a phishing email campaign that compromised several employee email account credentials. We write to provide you with information on the incident, steps the College is taking in response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate.

What Happened? On October 19, 2018, the College learned of suspicious activity related to certain employees' email accounts. We immediately launched an investigation to determine the full nature and scope of this incident. Through its detailed and exhaustive investigation, the College confirmed that an unknown actor(s) gained access to certain College employee email accounts as the result of a phishing attack against the email accounts. The employees' email credentials were changed, and the email accounts have been secured. A leading forensic investigation firm was immediately retained to assist with the College's investigation into what happened and what information contained within the email accounts may be affected. The investigation determined that an unknown individual had accessed certain College employees' email accounts between May 5, 2018 and November 5, 2018.

The contents of the accounts were reviewed through a manual and programmatic process to determine what sensitive data may have been accessible. On January 7, 2019, we confirmed the identities of the individuals who may have had information accessible as a result of the incident and promptly launched a review of our files to ascertain address information for the impacted individuals.

What Information Was Involved? While we have no evidence that your information was subject to actual or attempted misuse, we confirmed that your <<ClientDef1(name and [DATA ELEMENTS])>><<ClientDef2([DATA ELEMENTS])>> were contained within the affected employee email accounts.

What is Florida Keys Community College Doing? The College takes the security of personal information in our care very seriously. Upon learning of this event, we promptly notified potentially affected employees and worked with them to secure their relevant College accounts. The College has security measures in place to protect data in its care and is taking steps to enhance data security protections to protect against similar incidents in the future including implementing increased security measures for account access. We implemented Multi Factor Authentication on all email accounts to prevent unauthorized access without verification by the account owner. We are also notifying state and federal regulators as required by law.

As an added precaution, we secured the services of Kroll to provide identity monitoring services for 1 year at no cost to you. 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. Please review the instructions contained in the attached "Steps You Can Take to Protect Your Information" to enroll and receive these services. The cost of this service will be paid for by the College. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

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 contact 1-833-231-3356, Monday through Friday, 9:00 a.m. to 6:30 p.m., EST. You may also write to us at 5901 College Rd., Key West, FL 33040

The College takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Jonathan Gueverra
President
Florida Keys Community College

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **May 28, 2019** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-833-231-3356. Additional information describing your services is included with this letter.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226; 1-919-716-6400; and www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting 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.

Kroll

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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 can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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.

EXHIBIT B

Florida Keys Community College Provides Notice of Data Security Incident

Key West, Florida, February 27, 2019 – Florida Keys Community College (the "College") is taking action after discovering that it became the target of a phishing email campaign that compromised several employee email account credentials.

What Happened? On October 19, 2018 Florida Keys Community College (the "College") learned of suspicious activity regarding an employee's email account. We immediately launched an investigation, which included working with third-party forensic investigators, to determine the full nature and scope of this incident. The investigation determined that an unknown individual had accessed certain College employees' email accounts between May 5, 2018 and November 5, 2018.

The contents of the accounts were reviewed through a manual and programmatic process to determine what sensitive data may have been accessible. On January 7, 2019, we confirmed the identities of the individuals who may have had information accessible as a result of the incident and promptly launched a review of our files to ascertain address information for the impacted individuals.

What Information Was Involved? The investigation in this matter confirmed that some combination of the following types of personal information may have been accessible as a result of the incident: name, address, date of birth, Social Security number, passport information, medical information, and username and password.

What is Florida Keys Community College Doing? The College takes the security of personal information in our care very seriously. Upon learning of this event, we promptly notified potentially affected employees and worked with them to secure their relevant College accounts. We are notifying state regulators as required by law. We are notifying potentially affected individuals and will be offering these individuals access to 12 months of free identity protection services and providing additional information on steps to protect their identity.

The College has security measures in place to protect data in its care and is taking steps to enhance data security protections to protect against similar incidents in the future including implementing increased security measures for account access. We implemented Multi Factor Authentication on all email accounts to prevent unauthorized access to accounts without verification by the account owner.

For More Information The College established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. For additional information, please call 1-833-231-3356, Monday through Friday, 9:00 a.m. to 6:30 p.m., EST. You may also write to us at 5901 College Rd., Key West, FL 33040.

Monitor Your Accounts

The College encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without

your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.