NORTH ORANGE COUNTY
COMMUNITY COLLEGE DISTRICT

P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-783-1440
Or Visit:
https://response.idx.us/nocccd
Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: June 24, 2022

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

March 25, 2022

Notice of <<Variable Data 1>>

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

North Orange County Community College District ("NOCCCD") is writing to make you aware of an incident that may affect the privacy of some of your personal information. While we are unaware of any actual misuse of your information, safeguarding information is among NOCCCD's highest priorities, and this letter provides details of the incident, our response to it, and resources available to you right now to help protect your personal information, should you feel it is appropriate to do so.

What Happened? On January 10, 2022, NOCCCD became aware of suspicious activity on both Cypress College's and Fullerton College's networks. We began investigating the activity with the assistance of outside computer forensic specialists to determine the nature and scope of the incident. We have learned there was unauthorized access to certain systems between approximately December 7, 2021 and January 10, 2022, and that files containing sensitive information may have been taken/or viewed during that time by an unauthorized individual.

What Information Was Involved? Our investigation determined the following types of your information may have been impacted by this incident: name and <<Variable Data 2 >>.

What We Are Doing. Information security is among NOCCCD's highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to confirm the security of our systems, including the deployment of an advanced threat protection and monitoring tool. Additionally, we have implemented cybersecurity measures, such as multi-factor authentication, to further protect against similar incidents moving forward. We reported this incident to law enforcement and are cooperating with their investigation. We are notifying impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so. We are also reporting to regulatory authorities and the major credit reporting agencies, as required.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for <<12/24>> months at no cost to you, through IDX. You can find information on how to enroll in these services in the below "*Steps You Can Take to Help Protect Your Personal Information.*" We encourage you to enroll in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements 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 Protect Help 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 1-833-783-1440 between the hours of 6 am to 6 pm PT Monday through Friday. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Dr. Cherry Li-Bugg

Vice Chancellor, Educational Services and Technology
North Orange County Community College District

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

1. **Website and Enrollment**. Go to https://response.idx.us/nocccd and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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. *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 1-833-783-1440 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

IDX Identity will include one-year enrollments into the following service components:

1. SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.
2. CYBERSCAN - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like Social Security numbers, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.
3. IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible.
4. FULLY-MANAGED IDENTITY RECOVERY - IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned ID Care Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 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 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 your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report. To request a credit freeze, you will need to provide 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 you are a victim of identity theft.

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. NOCCCD is located at 1830 W. Romneya Drive, Anaheim, CA 92801-1819

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 bureaus 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.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<#>> Rhode Island residents impacted by this incident.

Dear Staff/Faculty – I am writing to notify you that the North Orange County Community College District ("NOCCCD") experienced a cybersecurity incident that affected the Cypress College and Fullerton College networks, and may have impacted the security of staff and faculty information across NOCCCD and **all** member sites (Cypress College, Fullerton College, North Orange Continuing Education, and District Services). We know there are concerns around this issue, as cyber security continues to be a challenge for many educational institutions and corporations. Please rest assured that the team has been working on this matter intently and we will be able to provide you with additional updates soon. Data security and information privacy are of the highest priority to NOCCCD, so we are reaching out to all current staff and faculty to provide information about the incident, the steps we are taking in response, and steps that any concerned individual can take to protect themselves, should they feel it appropriate.

If our ongoing review identifies you as potentially impacted, you will receive a separate communication with additional details as soon as possible. We appreciate your patience as we prepare that step and encourage you to review the below information and direct all questions and concerns to the phone number provided below.

What Happened? On January 10, 2022, NOCCCD became aware of suspicious activity on Cypress College's and Fullerton College's networks. We began investigating the activity with the assistance of outside computer forensic specialists to determine the nature and scope of the incident. Although our investigation is ongoing, we have learned that an unauthorized actor accessed both colleges' networks at varying times between approximately December 7, 2021 and January 10, 2022. Files containing employment-related information for faculty and staff may have been viewed or taken by the unauthorized actor.

What Information Was Involved? We are undertaking a thorough review with assistance from both internal college resources and outside specialists to better understand the individuals impacted and the types of information involved. If we determine that your information is at risk, NOCCCD will mail you a letter providing additional detail about the types of information involved, as well as complimentary credit monitoring and identity protection services as soon as possible.

What Is NOCCCD Doing? Upon becoming aware of this issue, we launched a response to secure our network, restore college operations, and investigate what happened. We are also coordinating with the colleges to review and enhance existing policies related to data protection and are working to implement multi-factor authentication to better protect data. We are reporting this incident to relevant regulators, as appropriate. We reported this incident to the FBI.

Why Was I Not Informed Sooner? NOCCCD immediately launched an investigation into the extent of the incident. While NOCCCD became aware of the incident on January 10, 2022, it took time to determine what information was impacted.

What Can Affected Individuals Do? We encourage you to review the below, *Steps You Can Take to Help Protect Your Personal Information.*

For More Information. We understand you may have additional questions concerning this incident. Individuals can direct questions to the telephone number **1-833-783-1440**: Monday through Friday from 6 am to 6 pm PT beginning on **Friday, February 18, 2022**. Please do not contact NOCCCD or the colleges directly as you will be referred back to the help line which is dedicated to answering all questions related to the incident.

Regards,

Byron D. Clift Breland, Ph.D.
Chancellor
North Orange County Community College District
1830 W. Romneya Drive Anaheim, CA 92801
www.nocccd.edu

NORTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT
Cypress College Fullerton College NOCE NORTH ORANGE CONTINUING EDUCATION

Steps You Can Take to Help Protect Your Personal Information

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 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 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 your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report. To request a credit freeze, you will need to provide 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 you are a victim of identity theft.

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 and your state Attorney General. This notice has not been delayed by law enforcement.

Dear Students,

We are writing to notify you that Cypress College recently experienced a cybersecurity incident that potentially impacted the security of certain student information kept on our network. At this time, we are continuing to investigate to determine which students were potentially impacted, and **we have not determined that all Cypress College students were impacted**. The security of our computer network and the student information we hold is of the highest priority to us, so we are reaching out to all current students now to provide information about the incident, the steps we are taking in response, and steps that any concerned individual can take to protect themself, should they feel it appropriate.

If our ongoing review identifies you as a potentially impacted student, you will receive an additional communication with additional details as soon as possible.

What Happened? On January 10, 2022, Cypress College identified suspicious activity on our computer network. We began investigating the activity with the assistance of outside computer forensic specialists to determine the nature and scope of the incident. Although our investigation is ongoing, we have so far learned that an unauthorized actor accessed our network between approximately December 7, 2021 and January 10, 2022. Files containing information for certain students may have been viewed and/or taken by the unauthorized actor.

What Information Was Involved? We are undertaking a thorough review with assistance from both internal college resources and outside specialists to better understand which students' information may have been impacted and the types of information involved. If we determine that your information is at risk Cypress College will mail you a letter providing additional detail about the types of information involved, as well as complimentary credit monitoring and identity protection services as soon as possible.

What Is Cypress College Doing? Upon becoming aware of this issue, we launched a response to secure our network, restore college operations, and investigate what happened. We are also reviewing and enhancing existing policies related to data protection. We are reporting this incident to relevant regulators, as appropriate. We reported this incident to the FBI.

What Can Affected Individuals Do? Although we have no indication at this time that all students receiving this notice were impacted by this incident, we do encourage everyone to review the below, *Steps You Can Take to Help Protect Your Personal Information.*

For More Information. We understand you may have additional questions concerning this incident. Individuals can direct questions to the telephone number **1-833-783-1440**: Monday through Friday from 6 am to 6 pm PT beginning on **Friday, February 18, 2022**. Please do not contact NOCCCD or the colleges directly as you will be referred back to the help line which is dedicated to answering all questions related to the incident.

Steps You Can Take to Help Protect Your Personal Information

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 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 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 your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report. To request a credit freeze, you will need to provide 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 you are a victim of identity theft.

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 and your state Attorney General. This notice has not been delayed by law enforcement.