

EXHIBIT 1

The investigation into this event is ongoing, and this notice will be supplemented with any substantive facts learned subsequent to its submission. By providing this notice, California College of the Arts (the “College”), does not waive any rights or defenses regarding the applicability of California law or personal jurisdiction.

Nature of the Data Event

On Friday January 19, 2018, a College laptop used by an employee was stolen out of the employee’s vehicle. The employee promptly reported the theft to College staff and to local law enforcement. The College quickly began to investigate and take steps to respond. The user’s passwords were changed to prevent access to the College’s computer systems. The College also began to monitor for signs that the laptop was active to remotely wipe the device. To date, the College has not seen any signs that laptop has connected to the internet. Since learning of the theft, the College has been identifying and reviewing files that may have been contained on the laptop at the time of the theft to determine what information may have been accessible on the device. To date, the investigation has found no evidence of any actual or attempted misuse of information as a result of this incident.

The investigation has determined that files on the laptop may have contained some combination of an individual’s name, Social Security number, date of birth, subscriber member number and/or health insurance information.

Notice to California Residents

On or around February 26, 2018, the College will begin providing written notice of this incident to individuals whose data may have been present on the stolen laptop, which includes two thousand five hundred eighty-one (2,581) California residents. Written notice will be provided in substantially the same form as the letter attached here as *Exhibit A*. On February 26, 2018, the College will also be providing notice of this incident to state-wide media in California. This notice will be provided in substantially the same form as the document attached here as *Exhibit B*.

Other Steps Taken and To Be Taken

Since discovering the theft, the College has worked diligently to determine what information may have been on the laptop and who may be impacted as a result of this crime. This process included consultation with third party firms that focus on cybersecurity issues to assist in the investigation. The College has taken steps to prevent further access from the laptop to the College’s systems. In addition to the internal investigation and efforts, the College continues to cooperate with law enforcement’s investigation.

The College is also providing written notice to those individuals whose data may have been present on the laptop at the time of the theft. This notice will include an offer of complimentary access to one (1) year of credit and identity monitoring services, including identity restoration services, through AllClear ID, and the contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, the College is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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. College will also be providing notice of this event to other entities as may be required under the applicable state laws.

EXHIBIT A



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

February 26, 2018

RE: NOTICE OF DATA BREACH

Dear John Sample:

We write regarding a recent incident that may affect the security of certain personal information related to you. We want to provide you with information about this incident, our response and steps you can take to protect against identity theft and fraud, should you feel it necessary to do so.

What Happened? On Friday January 19, 2018, a California College of Arts (the “College”) laptop used by one of our employees was stolen out of the employee’s vehicle. The employee promptly reported the theft to College staff and to local law enforcement. The College quickly began to investigate and take steps to respond. The user’s passwords were changed to prevent access to the College’s computer systems. The College also began to monitor for signs that the laptop was active to remotely wipe the device. To date, the College has not seen any signs that laptop has connected to the internet. Since learning of the theft, the College has been identifying and reviewing files that may have been contained on the laptop at the time of the theft to determine what information may have been accessible on the device. To date, we have no evidence of any actual or attempted misuse of information as a result of this incident.

What Information Was Involved? The investigation has determined that the following information related to you may have been on the laptop: name, Social Security number. We will be notifying all impacted individuals separately, so if your spouse and/or dependent are impacted, they will receive a separate letter of notification.

What We Are Doing. Since discovering the theft, we have worked diligently to determine what information may have been on the laptop and who may be impacted as a result of the crime. This process included consultation with third party firms that focus on cybersecurity issues to assist in the investigation. We have taken steps to prevent further access from the laptop to the College’s systems. In addition to our internal investigation and efforts, we continue to cooperate with law enforcement’s investigation. We will also be providing notice of this incident to state regulators as required.

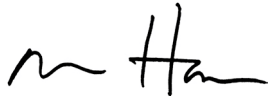
While we have no evidence of any actual or attempted misuse of information on the laptop, in an abundance of caution, we are offering you access to 12 months of credit monitoring and identity theft restoration services through AllClear ID at no cost to you.



What You Can Do. You can review the enclosed “Steps You Can Take to Protect Your Information,” which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft. You can also enroll in the credit monitoring and identity theft restoration services we are offering at no cost to you.

For More Information. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated call center we have established regarding this incident at 1-855-904-5760. The call center is available Monday through Saturday, 6:00 a.m. to 6:00 p.m. P.S.T (excluding U.S. holidays). We sincerely regret any inconvenience or undue concern this incident has caused you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Mara Hancock', written in a cursive style.

Mara Hancock
CIO, VP-Technology
California College of Arts

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

While we have no evidence of actual or attempted misuse of personal information, as an added precaution, we have arranged to have AllClear ID protect your identity for twelve (12) 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 twelve (12) months:

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-904-5760 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of public databases for use of your child's information. To enroll in this 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 1-855-904-5760 using the following redemption code: Redemption Code.

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

Monitor Your Accounts

Credit Reports. 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. 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.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com



Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting 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 encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

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

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

For Rhode Island residents, the Rhode Island Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 2 Rhode Island residents are potentially impacted by this incident. You have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim.

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 a 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.





00029
ACD1234

02701
TO THE PARENT OR GUARDIAN OF
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

February 26, 2018

RE: NOTICE OF DATA BREACH

Dear Parent or Guardian of John Sample:

We write regarding a recent incident that may affect the security of certain personal information related to your minor. We want to provide you with information about this incident, our response and steps you can take to protect against identity theft and fraud, should you feel it necessary to do so.

What Happened? On Friday January 19, 2018, a California College of Arts (the “College”) laptop used by one of our employees was stolen out of the employee’s vehicle. The employee promptly reported the theft to College staff and to local law enforcement. The College quickly began to investigate and take steps to respond. The user’s passwords were changed to prevent access to the College’s computer systems. The College also began to monitor for signs that the laptop was active to remotely wipe the device. To date, the College has not seen any signs that laptop has connected to the internet. Since learning of the theft, the College has been identifying and reviewing files that may have been contained on the laptop at the time of the theft to determine what information may have been accessible on the device. To date, we have no evidence of any actual or attempted misuse of information as a result of this incident.

What Information Was Involved? The investigation has determined that the following information related to your minor may have been on the laptop: name, health insurance information, health insurance number, dental insurance information. We will be notifying all impacted individuals separately, so if you and/or your spouse are impacted, you and/or they will receive a separate letter of notification.

What We Are Doing. Since discovering the theft, we have worked diligently to determine what information may have been on the laptop and who may be impacted as a result of the crime. This process included consultation with third party firms that focus on cybersecurity issues to assist in the investigation. We have taken steps to prevent further access from the laptop to the College’s systems. In addition to our internal investigation and efforts, we continue to cooperate with law enforcement’s investigation. We will also be providing notice of this incident to state regulators as required.

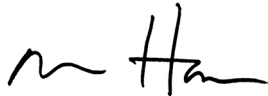
While we have no evidence of any actual or attempted misuse of information on the laptop, in an abundance of caution, we are offering your minor access to 12 months of identity theft protection services through AllClear ID at no cost to you.



What You Can Do. You can review the enclosed “Steps You Can Take to Protect Personal Information,” which includes guidance on steps an individual can take to better protect against the possibility of fraud and identify theft. You can also enroll your minor in the identity theft protection services we are offering at no cost to you.

For More Information. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated call center we have established regarding this incident at 1-855-904-5760. The call center is available Monday through Saturday, 6:00 a.m. to 6:00 p.m. P.S.T (excluding U.S. holidays). We sincerely regret any inconvenience or undue concern this incident has caused you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Mara Hancock', with a stylized, cursive script.

Mara Hancock
CIO, VP-Technology
California College of Arts

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

While we have no evidence of actual or attempted misuse of personal information, as an added precaution, we have arranged to have AllClear ID protect your minor's identity for twelve (12) months at no cost to you. The following identity protection services start on the date of this notice and can be used them at any time during the next twelve (12) months:

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-904-5760 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of public databases for use of your child's information. To enroll in this 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 1-855-904-5760 using the following redemption code: Redemption Code.

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

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your minor's account statements and monitoring your minor's free credit reports, if available, for suspicious activity and to detect errors. While children under 18 years old do not have credit files, the following information relates to protecting one's credit once established:

Credit Reports. Under U.S. law, adults are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. An individual may also contact the three major credit bureaus directly to request a free copy of a credit report.

Fraud Alerts. At no charge, individuals can also have these credit bureaus place a "fraud alert" on a credit file that alerts creditors to take additional steps to verify identity prior to granting credit in the individual's name. Note, however, that because it tells creditors to follow certain procedures to protect identity, it may also delay the ability to obtain credit while the agency verifies identity. As soon as one credit bureau confirms the fraud alert, the others are notified to place fraud alerts on the file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com



Security Freeze. Individuals may also place a security freeze on a credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on a credit report may delay, interfere with, or prevent the timely approval of any requests made for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. An individual must place a security freeze separately with each of the three major credit bureaus listed above in order to place a freeze on all credit files. In order to request a security freeze, the credit bureau will require full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of a state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect your minor against identity theft and fraud by contacting 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 encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

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

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

For Rhode Island residents, the Rhode Island Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 2 Rhode Island residents are potentially impacted by this incident. An individual has the right to file and obtain a police report if he or she ever experiences identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, the law enforcement agency will likely require some kind of proof that the individual has been a victim.

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 a 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.



EXHIBIT B

NOTICE TO MEDIA

FOR IMMEDIATE RELEASE

RE: California College of Arts, Notice of Data Security Incident

San Francisco, California (February 26, 2018) – On Friday January 19, 2018, a California College of Arts (the “College”) laptop used by one of our employees was stolen out of the employee’s vehicle. The employee promptly reported the theft to College staff and to local law enforcement. The College quickly began to investigate and take steps to respond. The user’s passwords were changed to prevent access to the College’s computer systems. The College also began to monitor for signs that the laptop was active to remotely wipe the device. To date, the College has not seen any signs that laptop has connected to the internet. Since learning of the theft, the College has been identifying and reviewing files that may have been contained on the laptop at the time of the theft to determine what information may have been accessible on the device. The investigation has determined that files on the laptop may have contained some combination of an individual’s name, Social Security number, date of birth, subscriber member number and/or health insurance information.

To date, the College has no evidence of any actual or attempted misuse of information as a result of this incident.

Since discovering the theft, the College has worked diligently to determine what information may have been on the laptop and who may be impacted as a result of the crime. On February 26, 2018, the College mailed notice letters to all individuals who may have been affected by this incident. The College has offered potentially impacted individuals access to credit monitoring and identity restoration services for one year without charge. The College is encouraging potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports and explanation of benefits forms for suspicious activity. The College’s notification to potentially impacted individuals includes information on obtaining a free credit report annually from each of the three major credit reporting bureaus by visiting www.annualcreditreport.com, calling 877-322-8228, or contacting the three major credit bureaus directly at: **Equifax**, P.O. Box 105069, Atlanta, GA, 30348, 800-525-6285, www.equifax.com; **Experian**, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; **TransUnion**, P.O. Box 2000, Chester, PA 19016, 800-680-7289, www.transunion.com. Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, the Federal Trade Commission or their 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. Instances of known or suspected identity theft should also be reported to law enforcement or the individual’s state Attorney General. The College has provided notice of this incident to the U.S. Department of Health and Human Services, as well as required state regulators. This incident has also been reported to law enforcement.

The College has set up a call center to answer questions from those notified of this incident. The dedicated assistance line may be reached at 1-855-904-5760, Monday through Saturday, 6:00 a.m. to 6:00 p.m. P.S.T (excluding U.S. holidays).