Logo/Client Name
C/O ID Experts
<<Return Address>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
[TFN]
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

The privacy and security of your personal information is extremely important to the University of California. We are writing to inform you of a security matter involving some of your personal information and to advise you of steps you can take to protect your privacy.

What Happened

On June 1, 2020, the University of California San Francisco ("UCSF") detected a cybersecurity attack that occurred in a limited part of the UCSF School of Medicine's IT environment. Upon detection of the intrusion, we immediately isolated the impacted environment and successfully contained the incident from the core UCSF network. While we stopped the attack as it was occurring, the attacker obtained certain files and encrypted others with ransomware. UCSF made the difficult decision to pay the attacker, and received the information we needed to decrypt the affected servers and data the attackers stole. Although we have no evidence that the personal information taken has been misused, we are notifying you because we determined that some of your personal information was impacted.

What Information Was Involved

The personal information impacted could have included:

- your name and your social security number. It did not contain any of your financial information.
- your name, social security number, financial information, and some personal information.
- your name, social security number, and some health information. It did not contain any of your financial information.
- your name, social security number, and some health insurance information.
- your name, social security number, and some other personal information. It did not contain any financial information.
- your name, social security number, government identification, and some other personal information. It did not contain any financial information.
- your name, social security number, government identification, and some financial information.
- your name and some of your medical information. It did not contain your social security number or any financial information.
- your name, government identification, financial information, and some other information. It did not contain your social security number.
- your name, government identification, and some other information. It did not contain your social security number or any financial information.
- your name, medical information, and some other information. It did not contain your social security number or any financial information. your name, social security number, and some other personal or financial information.

What We Are Doing

UCSF is committed to maintaining the privacy and security of personal information. In response to this incident, UCSF immediately notified law enforcement and retained a leading data security firm to assist in investigating the incident. UCSF also launched a thorough investigation and began implementation of a number of enhancements to our security and privacy program to help reduce the risk of this kind of incident from happening again. This includes strengthening existing controls, data backup, user training and awareness, and other measures.

Although there are no indications that personal data implicated by this situation has been misused, as an added precaution, we are also offering you complimentary access to 12 months of credit monitoring and identity theft restoration services through IDX, the data breach and recovery services expert. We encourage you to enroll in these services. Please review the instructions contained in the attached "Recommended Steps to Protect Your Information" for additional information.

What You Can Do

We are bringing this incident to your attention so you can be vigilant to signs of possible misuse of your personal information or identity. Please note that UCSF will not contact you again in relation to this incident, so if an unknown person should contact you to confirm any of your personal information, do not provide any details.

We also encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is January 21, 2021.

IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

We regret this occurred. Should you have any questions about this matter or require assistance, please contact ID Experts with any questions by calling 1-800-939-4170 or go to https://app.idx.us/account-creation/protect.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

MyIDCare™

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://app.myidcare.com/account-creation/protect 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 MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at [TFN] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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.

You should also know that you have the right to file a police report if you ever experience identity 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. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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. You can 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.