UNIVERSITY OF CALIFORNIA, SANTA CRUZ

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

Student Health Services
Cowell Student Health Center
1156 High Street
Santa Cruz, CA 95064

PH (831) 459-2869
(831) 459-2211
FAX (831) 459-4330

April 21, 2017

Dear UC SHIP Student,

We are writing with important information about a fraud scheme targeting UC SHIP members. We do not have information at this time indicating that you have been impacted by this scheme. But we are sharing this information out of caution to assist our students in protecting themselves and their health information, as we have information that the perpetrators of this scheme are actively soliciting UC students in variety of ways to obtain their UC SHIP membership information. This letter contains important information about how to protect your health information and your identity.

How the Scheme Works

We recently received information that a non-UC provider has been contacting students under suspicious pretenses to obtain their UC SHIP membership information and then using their UC SHIP numbers to prescribe multiple medications to those students.

- We have been informed that a company called "California Clinical Trials LLC" is specifically advertising to students enrolled in UC SHIP to enroll them in a "clinical trial" of topical pain creams. These ads have appeared on Facebook and have offered UC SHIP members up to $550 to enroll in their "clinical trial." We believe that students may have been misled into believing that this "clinical trial" was associated with UC SHIP, which it is not. This company and its activities have absolutely no relationship to the University of California.

- We understand that a company called "PharmaPro Solutions" has appeared at job or recruiting fairs to solicit UC students to apply for jobs as sales representatives. As part of the "employment application," we understand that PharmaPro representatives have asked students to provide UC SHIP insurance numbers and other health information. The student shortly thereafter begins to receive prescription topical pain creams in the mail from a mail-order pharmacy, even though the student did not ask for the prescription and did not consult with a doctor or pharmacist. This company and its activities have absolutely no relationship to the University of California.

- Lastly, we believe that PharmaPro Solutions or another company may be tabling or setting up unauthorized booths at or around UC campuses and offering "free samples" of these topical pain creams. In exchange for the sample, the company is believed to be requesting UC SHIP membership information. Again, these activities have absolutely no relationship to the University of California.

We believe that, once students' UC SHIP membership information is collected, the scheme involves writing large numbers of fraudulent prescriptions for topical pain medications in the names of these students. The prescription medications involved include Dermacin, Inflammacin, Diclofex, Mebolic, Migranow, Inflammation Reduction Pak, Xelitral, and possibly others. Most of these medications are packaged in kits consisting of a drug similar to ibuprofen (either as a topical solution or as pills), coupled with a second component, which is similar to an over-the-counter "Ben-Gay" or "Icy-Hot" cream. Mebolic is a prescription vitamin product, and Migranow is a kit composed of a generic migraine medication plus a topical cooling liquid similar to over-the-counter "Vic's VapoRub."

What We Are Doing

We consider this matter fraud against our students and the University, and are taking every reasonable step to protect our students and the UC SHIP plan from this kind of abuse. UC SHIP itself uncovered this scheme and is conducting an in-depth, ongoing investigation with our legal counsel and law enforcement. We have taken immediate actions to cut-off the prescribers and all the companies and persons known to us who may be involved in this scheme, including suspending participation of such providers and pharmacies in our plan, effective immediately. We are taking additional, preventive actions with respect to the high-cost drugs and kits involved here that are an emerging target for fraud and are placing additional internal controls around UC SHIP claims. We are actively pursuing legal action and working with law enforcement to hold the perpetrators accountable.

If you have information that may assist law enforcement or the University in this matter, please contact the UCSC Police Department at (831) 459-2231 ext. 1

Protecting Yourself and Your Information

This scheme appears sophisticated and our investigation remains active, so we do not know all of the facts at this time. We are contacting you now because your well-being and privacy are paramount. We encourage you to observe the following tips to keep yourself and your information safe:

1) Beware of so-called "clinical trials" advertised on social media, the web, and elsewhere. Some of these clinical trials are shams, designed to leverage your UC SHIP coverage to write expensive prescriptions for what are essentially worthless medications. These medications may even be dangerous. The University strongly encourages students and third parties to verify a researcher's credentials and affiliation before participating in any clinical trial. Make sure that the informed consent form you sign lists an Institutional Review Board, or Ethics Committee, and contact them to make sure the study is legitimate. Information about legitimate clinical trials can also be found at www.clinicaltrials.gov. UC runs many clinical trials, and they are absolutely essential to ensuring the advancement of medicine. A genuine clinical trial has important protections for its enrollees. A true clinical trial will rarely offer large sums of money for participants.

2) Do not share your UC SHIP membership information with anyone, other than your health care provider; when in doubt, check with your Student Health Center. Your membership number is private, sensitive information. Do not share it with organizations tabling on campus or as part of an employment application. In California, employers can only ask for medical or health insurance information in limited circumstances and very rarely when you are first applying for a job.

We also want to alert you to resources for protecting your identity. Please find enclosed important information about checking your credit reports and ensuring that no new accounts were created in your name. Students enrolled in UC SHIP also have access to **AllClear ID** via Anthem. Students can contact **AllClear ID** at https://anthemcares.allclearid.com, or 1-855-227-9830, (Monday through Saturday from 8:00 AM - 8:00 PM Central Time). Services include the following:

- **Identity Theft Repair Assistance:** Should a student experience fraud, an investigator will do the work to recover financial losses, restore the student's credit, and ensure the student's identity is returned to its proper condition. This assistance will cover any fraud that has occurred since the incident first began.

- **Credit Monitoring:** At no cost, students may also enroll in additional protections, including credit monitoring. Credit monitoring alerts consumers when banks and creditors use their identity to open new credit accounts.

- **Child Identity Protection**: Child-specific identity protection services will also be offered to any students with children insured through their Anthem plan.

- **Identity theft insurance:** For individuals who enroll, the company has arranged for $1,000,000 in identity theft insurance, where allowed by law.

- **Identity theft monitoring/fraud detection:** For students who enroll, data such as credit card numbers, Social Security numbers and emails will be scanned against aggregated data sources maintained by top security researchers that contain stolen and compromised individual data, in order to look for any indication that the students' data has been compromised.

- **Phone Alerts:** Individuals who register for this service and provide their contact information will receive an alert when there is a notification from a credit bureau, or when it appears from identity theft monitoring

Finally, we want to take this opportunity to remind you that it is important that you protect your personally identifying information (health insurance ID, Social Security number, bank account information, etc.) at all times from unauthorized use. Your health plan information and medical identity can be valuable to an identity thief. As a result, please take precautions including:

- You should never provide your health insurance ID or Social Security number to someone you don't know. Also, as a rule, avoid sharing sensitive information over email or through social media.

- Be wary if someone offers you "free" health services or products, but requires you to provide your health plan ID number. Medical identity thieves may pretend to work for an insurance company, doctors' offices, clinic, or pharmacy to try to trick you into revealing sensitive information.

- Keep paper and electronic copies of your medical and health insurance records in a safe place. Shred outdated health insurance forms, prescription and physician statements, and the labels from prescription bottles before you throw them out.

- Before you provide sensitive personal information to a website that asks for your social security number, insurance account numbers, or details about your health, find out why the information is needed, how it will be kept safe, whether it will be shared, and with whom. If you decide to share your information online, first read the privacy policy on the website and look for a lock icon on the browser's status bar or a URL that begins "https:" the "s" is for secure.

We appreciate your attention to this important matter.

For further information and updates go to:

http://healthcenter.ucsc.edu/news-events/news/ucship_members.html or call 831-502-7955

Sincerely,

Mary Knudtson, DNSc, NP, FAAN
Executive Director Student Health Services UCSC

Jaye Padgett, PhD
Interim Vice Provost for Student Success UCSC

Information about Identity Theft Prevention

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report once every 12 months by requesting your report online at www.annualcreditreport.com, calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below.

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

If you discover any suspicious activity, notify ID Experts® and file a theft report. You will be contacted by a member of the ID Experts® Recovery Department. If you are a victim of identity theft, you will be assigned an ID Experts® Recovery Advocate who will work on your behalf to identify, stop, and reverse the damage quickly.

You should also report a suspected incident of identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW Washington, DC 20580; 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

You may obtain information from the FTC and the consumer reporting agencies listed above about fraud alerts and credit freezes. We provide some additional information about fraud alerts and credit freezes below.

Fraud Alerts: There are 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 (7) 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 above. Once you have requested an alert with one credit reporting agency, your request will automatically be sent to the other two agencies.

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 personal identification number (PIN) or password (or both) 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, temporarily lift, and/or permanently remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and permanently removing a credit freeze also varies by state (the cost is generally $5 to $20 per transaction at each credit reporting agency). *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting agency.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting agencies listed above to find out more information.