UNIVERSITY
OF
CALIFORNIA

Updated April 5, 2021

TO THE UNIVERSITY OF CALIFORNIA COMMUNITY

We are writing to provide you additional information about a data security incident affecting the UC community and what you should do to protect your personal information.

As was announced on March 31st, like several hundred other institutions throughout the country, including universities, government institutions and private companies, UC has been using a vendor service called Accellion File Transfer Appliance (FTA) to transfer information. Accellion was the target of an international cyber attack where the perpetrators exploited a vulnerability in Accellion's program and attacked roughly 100 organizations. The attackers are now attempting to get money from organizations and individuals.

We are working with local and federal law enforcement and third-party vendors to investigate this incident, to assess the information that has been compromised, to enforce the law, and to limit the release of stolen information.

We are alerting you now so you are able to take protective actions as we work to address the situation.

What you should do to protect your personal and financial information:

- *Sign up for free credit monitoring and identity theft protection*: To help you protect your identity, we are offering the entire UC community complimentary credit monitoring and identity theft protection for one year through Experian IdentityWorks^{SM}. This service includes:
    - *Credit monitoring:* Actively monitors your Experian file for indicators of fraud.
    - *Internet surveillance:* Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the dark web.
    - *Identity restoration:* Identity restoration specialists are immediately available to help you address credit and non-credit related fraud.
    - *Experian IdentityWorks ExtendCARETM:* You receive the same high-level of identity restoration support even after your Experian IdentityWorks membership has expired.

- ○ *$1 Million Identity Theft Insurance:* Provides coverage for certain costs and unauthorized electronic fund transfers.
- ○ *Lost wallet:* Provides assistance with canceling/replacing lost or stolen credit, debit, and medical cards.
- ○ *Child monitoring:* For 10 children up to 18 years old, internet surveillance and monitoring to determine whether enrolled minors in your household have an Experian credit report are available. Also included are identity restoration and up to $1M Identity Theft Insurance.

Sign up at the Experian IdentityWorks website using the enrollment code JCZGTC333:

- ○ For adults, visit experianidworks.com/RR3Bplus
- ○ For minors, visit experianidworks.com/minorplus

For help with enrolling, you may call (866) 617-1923 and reference engagement number DB26512.

- • *Monitor and set up alerts for bank account(s)*: Monitor your bank account(s) for suspicious transactions and report any to your bank. Ask the bank for online monitoring and alerts on your account. This will give you early warning of any fraudulent transactions.
- • *Watch out for suspicious emails:* We believe the person(s) behind the Accellion FTA attack may send threatening mass emails in an attempt to scare people into giving them money. Anyone receiving such an email should either forward it to your local information security office or simply delete it. Please do not engage or respond.
- • *Place a fraud alert on your credit file:* We recommend you place a fraud alert on your credit file by contacting one of the three nationwide credit bureaus listed below. If a fraud alert is placed on a consumer's credit file, certain identity verification steps must be taken prior to extending new credit.

- ○ https://www.equifax.com/personal/

UNIVERSITY
OF
CALIFORNIA

- ○ https://www.transunion.com
- ○ https://www.experian.com/

- *Important reminders about protecting yourself:* These incidents are reminders of the importance of doing everything possible to protect your online information. Here are five rules for protecting your information. In addition, you may wish to take additional identity theft measures described at https://www.identitytheft.gov/databreach

We regard the privacy of all of our community members with the utmost seriousness. We will keep the UC community updated as we learn more and are able to share additional information.

UNIVERSITY
OF
CALIFORNIA

Accellion Breach FAQs

Updated April 7, 2021

What happened - what is this about?

Like several hundred other institutions throughout the country, including universities, government institutions and private companies, UC has been using a vendor service called Accellion File Transfer Appliance (FTA) to transfer information. Accellion was the target of an international cyber attack where the perpetrators exploited a vulnerability in Accellion's program and attacked roughly 100 organizations. The attackers are now attempting to get money from organizations and individuals.

What kind of personal information was stolen?

At this time, we believe the stolen information includes but is not limited to names, addresses, telephone numbers, birth dates, Social Security numbers and bank account information for a range of UC populations, including employees and their dependents and beneficiaries, retirees and their beneficiaries, students and their families, and potentially other individuals with connections to UC.

How do I know if my information was involved?

We are investigating the incident and working to identify affected individuals. We will notify affected people and provide information regarding additional steps they can take to protect themselves. Meanwhile, UC recommends that all members of the UC community take immediate action to protect themselves, including signing up for UC's free credit monitoring and identity theft protection through Experian (at https://ucnet.universityofcalifornia.edu/ news/2021/04/update-on-accellion-breach-and-what-you-should-do.html).

What is UC doing to protect my data?

UC is conducting a thorough review of the security controls for centralized systems handling sensitive data, and we will be implementing additional security measures to prevent similar incidents in the future. We are also working with local and federal law enforcement and third-party vendors to investigate this incident, to assess the information that has been compromised, to enforce the law, and to limit the release of stolen information.

UNIVERSITY
OF
CALIFORNIA

Are my family members' information impacted?

Family members who are listed as dependents or beneficiaries on employee or retiree accounts, or who are listed on student paperwork, may be affected. Family members in these groups should take immediate action to protect themselves, including signing up for UC's free credit monitoring and identity theft protection through Experian (at https://ucnet.universityofcalifornia.edu/news/2021/04/update-on-accellion-breach-and-what-you-should-do.html).

Are my medical benefits impacted?

Your benefits are not impacted, but your personal information may be at risk. You are strongly encouraged to take immediate action to protect yourself, including signing up for UC's free credit monitoring and identity theft protection through Experian (at https://ucnet.universityofcalifornia.edu/news/2021/04/update-on-accellion-breach-and-what-you-should-do.html).

I am a UC retiree — is my pension impacted?

Your pension is not impacted, but your personal information may be at risk. You are strongly encouraged to take immediate action to protect yourself, including signing up for UC's free credit monitoring and identity theft protection through Experian (at https://ucnet.universityofcalifornia.edu/news/2021/04/update-on-accellion-breach-and-what-you-should-do.html).

How long will free credit monitoring and identity theft protection last?

The free credit monitoring and identity theft protection UC is offering its community members is good for one year.

How do I protect myself?

All members of the UC community are encouraged to sign up for free credit monitoring and identity theft protection through Experian (at https://ucnet.universityofcalifornia.edu/news/2021/04/update-on-accellion-breach-and-what-you-should-do.html). Additionally, here are five rules for protecting your information (at https://ucnet.universityofcalifornia.edu/news/2021/03/five-rules-for-protecting-your-security-online.html). You may also take additional identity theft measures described at https://www.identitytheft.gov/databreach.

How can I be sure the Experian site is secure and it's safe to provide Experian my personal information?

Information about Experian's security measures and tools is available on the Experian website (at https://www.experian.com/privacy/ask-experian-privacy-policy).

Why does the Experian website require my Social Security number and other personal information?

The Experian service also provides Internet-based identity monitoring in order to notify you if any of your personal information, such as your Social Security number, is found as being bought or sold online.

Is this attack real or another phishing scam?

As UC announced previously, this is a real and serious attack on Accellion that has impacted UC. All members of the UC community are strongly encouraged to take immediate action to protect themselves, including signing up for UC's free credit monitoring and identity theft protection through Experian (at https://ucnet.universityofcalifornia.edu/news/2021/04/ update-on-accellion-breach-and-what-you-should-do.html).

What should I do if I get an email or phone call asking me for money?

These types of messages should be immediately forwarded to your local information security office.

Is it safe to click on the links in these FAQs or the UC emails I receive?

Yes. If you have any questions whether a UC email, document or web page regarding this incident is legitimate, please contact your local information security office.

What should I do if I have questions?

Questions about this incident may be sent to communications@ucop.edu. We will address as many questions as possible in this FAQ.