UNIVERSITY
OF
CALIFORNIA

Watch out for suspicious solicitations for new bank accounts

UC has learned that names, Social Security numbers and other personal information of some members of the UC community may have been used in attempts to open unauthorized bank accounts at financial institutions such as Chime and Go2Bank. Some of these UC community members are receiving emails from these institutions asking them to confirm a new account by clicking on a link in the email. It is unclear how personal information was obtained to open unauthorized accounts.

UC has been in touch with both Chime and Go2Bank, and both companies are currently cooperating with UC to investigate this incident. It appears that personnel at other companies have also received similar emails from Chime and Go2Bank. Chime has closed some accounts and is researching whether other accounts are authorized or not. We are currently awaiting more information from Go2Bank.

What UC community members can do to protect themselves

- ***Watch out for communications from Chime/Go2Bank****:* Be on the lookout for email or physical mail notifications suggesting an account that you did not open. These may come in different forms — notification of a new account, requests to confirm your email address, or physical debit/credit cards sent to your home address.

  Anyone receiving an email from Chime or Go2Bank asking them to confirm a new bank account they do not recognize **should not click any links in the email, and should forward the email to their local information security office.

- ***Promptly close unauthorized accounts:*** If you believe an account has been opened without your permission, contact the company immediately and inform them you believe someone has fraudulently opened an account. Ask the company to close the account and confirm the closure with you once complete. Individuals may contact Chime at 844-244-6363 and support@chime.com. Individuals may contact Go2Bank at 855-459-1334 or by using one of the methods listed at https://www.go2bank.com/help/contact-us.

- ***Monitor and set up alerts for bank account(s)***: Monitor bank account(s) for suspicious transactions and report any to your bank. Ask the bank for online monitoring and alerts on your account.

- ***Place a fraud alert on your credit file****:* We recommend impacted individuals place a fraud alert on their 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/
  - https://www.transunion.com
  - https://www.experian.com/

- ***Sign up for credit monitoring****:* If you haven't already done so, we recommend impacted individuals sign up for the Experian credit monitoring service being offered by UC.

- ***Reminders for protecting personal information****:* Here are five rules for protecting your information. In addition, you may take additional identity theft measures described at https://www.identitytheft.gov/databreach

What UC is doing

UNIVERSITY
OF
CALIFORNIA

- We continue to communicate with Chime and Go2Bank to learn more about this incident, and work with them to monitor accounts associated with UC email addresses.
- We have contacted the relevant law enforcement agencies.
- We are monitoring systems to determine whether there are additional similar communications from these or other institutions.