Risk Alert Identity Theft and Cellphones

The Federal Communication Commission (FCC) defines cellular fraud as "the unauthorized use, tampering or manipulation of a cellular phone or service." The FCC has reported that of the 250,854 identity theft complaints reported in 2011, the wireless or cellphone category accounted for 3.7 percent, or 9,282, of them. Because the use of cellphones is escalating, it is likely the number of identity theft complaints will increase and fraudsters will continue to develop new cellphone scams that will increase the risk for everyone.

Smishing/Vishing Cellular Fraud

According to the FBI, a fraudster will send an alert or recorded phone message to a person saying that "Your ATM card needs to be reactivated". The message further instructs the individual to call a phone number or communicate in some way to correct the problem. The fraudster will then make contact and ask for personal identification numbers, account information and possibly credit card numbers. From this information, the fraudster can establish credit accounts in the victim's name or possibly access their account to make withdrawals and wire money to other financial institutions.

The FBI recently reported these examples of smishing scams:

- Account holders at a credit union, after receiving a text message about an account problem, called the phone number in the text, gave out personal information and had money withdrawn from their bank accounts within 10 minutes of their calls.
- Customers at a bank received a text saying they needed to reactivate their ATM cards. Some called the phone number in the text and were prompted to provide their ATM card numbers, PINs and expiration dates. Thousands of fraudulent withdrawals followed.

Subscriber Cellular Fraud

According to the FCC, subscriber cellular fraud is the "primary type of cell fraud," costing carriers more than $150 million per year. The scam originates when an individual fraudulently obtains personal information of victims and uses it to open up new cell phone accounts in the victims' names. Each victim, who ends up with two cell phone accounts, is charged for his or her legitimate calls and the fraudster's phone calls as well. The victims then have to try to disavow the bogus charges.

Cloning Cellular Fraud

Every cell phone is supposed to have a unique factory-set electronic serial number (ESN) and telephone number (MIN). A cloned cell phone is one that has been reprogrammed to transmit the ESN and MIN belonging to another (legitimate) cell phone. Fraudsters can obtain valid ESN/MIN combinations by illegally monitoring the radio wave transmissions from the cell phones of legitimate subscribers. After cloning, both the legitimate and the fraudulent cell phones have the same ESN/MIN combination and cellular systems cannot distinguish the cloned cell phone from the legitimate one. The legitimate phone user then gets billed for the cloned phone’s calls. Immediately notify your telephone carrier if you think you have been a victim of cloning fraud.

Prevention Tips for CU Members:

- Beware of these type fraud schemes and watch your accounts closely.
- Protect your personal information and never provide account information to someone you don't know or trust.
- To prevent subscriber fraud, make sure that your personal information is kept private when purchasing anything in a store or on the Internet.
- For cell phone cloning fraud, the cellular equipment manufacturing industry has deployed authentication systems that have proven to be a very effective countermeasure to cloning. If interested, call your cellular phone carrier for more information.