

RiskWatch Bulletin



July 2017

7-17

Social Engineering: Conditions of Coverage

Social Engineering is fraudulent impersonation in order to gain confidential information, achieve theft or accomplish other nefarious goals. This happened recently at Utah Agencies and Schools. These types of losses can be devastating and as expected, we and Starr Companies, our Crime/Fidelity Excess Carrier, are concerned. As a result, our self-insured retention (SIR) limit has moved up from \$500,000 to \$1,000,000. Moreover, each state agency, higher education institution and public K-12 school is required to do the following to help prevent further losses:

- Have a call-back, email, text or similar notification made by the state agency's/school's financial institution or banking partner within 24 hours, notifying the agency/school of all electronic transfers of funds.
- The agency/school will review the notification and contact its financial institution/banking partner within 24 hours of receipt, regarding any discrepancies or unrecognized transactions.
- The agency/school shall use antivirus software on all electronic devices, including desktops, portable computers, and mobile devices. The software will be updated in accordance with the software providers' recommendations.

To gain further understanding of these sorts of threats and how to protect against them, please expect to attend our next Risk Symposium on October 30th. A "Save the Date" will arrive shortly.

Brian Nelson, Risk Management Director



Trending Risks & Pending Concerns