Informed Investor Alert
SOCIAL NETWORKING

The Department of Business Regulation
CAUTIONS INVESTORS ABOUT SOCIAL NETWORKING FRAUD

August 28, 2013 – As people increasingly turn to online social networking sites to interact with one another, so have con artists who lurk in the virtual shadows with shady investment deals to pitch to unsuspecting investors, the Department of Business Regulation ("DBR") said today.

The DBR cautioned investors to make sure they know who they are doing business with when considering investments pitched through "friends" on social networking sites.

"Just because someone has 'friended' you online does not mean that person is your friend when it comes to investing," said Deputy Director Maria D'Alessandro "The person behind the profile may be deliberately mimicking your likes and interests to lure you into a scam."

Con artists have launched "affinity fraud" schemes for years by targeting victims through traditional offline social networks, such as community service groups, professional associations or faith-based organizations. Scammers infiltrate groups of individuals connected through common interests, hobbies, lifestyles, professions or faith to establish strong bonds through face-to-face contact and sharing of personal interests before launching their schemes.

The rise in popularity of websites such as Facebook, Twitter, LinkedIn, eHarmony and other online social networks and communities has made it easier for con artists to quickly establish trust and credibility. "Crooks peddling scams increasingly are logging on to find investors and their money," D'Alessandro said.

Online social networking sites enable scammers to gain access to potential victims through their online profiles, which may contain sensitive personal information such as their dates or places of birth, phone numbers, home addresses, religious and political views, employment histories, and even personal photographs.

"A con artist can take advantage of how easily people share background and personal information online by using this information to make a highly targeted pitch to "friends" within that social group," D'Alessandro said.

The alert advises investors to watch for red flags common to online investment schemes, such as promises of high returns with no risk, operations based offshore and requests for payment through e-currency websites. The alert also offers tips on how to protect against fraud in social networking: protect your personal information; search the names of all persons and companies connected to the investment being offered; beware of the use of testimonials from "satisfied" investors; obtain a prospectus; don't take the word of a salesperson; and contact the DBR to determine if the investment and the person recommending it are properly registered.

"Take time to check out the investment yourself, and remember: If it sounds too good to be true, it probably is," D'Alessandro said.

The alert is available online at:
http://www.dbr.ri.gov/documents/divisions/banking/securities/SD-Investor_Alert-Social_Networking.pdf. For more information, contact the Securities Division of the Department of Business Regulation at securitiesinquiry@dbr.ri.gov or by phone (401) 462-9500.