



**Contact:**

**James Burns**  
Bureau Chief  
Securities Bureau  
(208) 332-8080

## NEWS RELEASE

**For Immediate Release**

**January 28, 2015**

### ***DEPARTMENT OF FINANCE REMINDS INVESTORS TO DISCUSS CYBERSECURITY WITH THEIR FINANCIAL PROFESSIONALS***

Boise, Idaho – – With an ever-growing list of financial service providers and other companies targeted by organized cyber-attacks, the Idaho Department of Finance today issued an advisory reminding investors of the importance of understanding how their personal information is being protected by financial firms. The advisory is on the department's website at <http://www.finance.idaho.gov>.

"Our increasing use of and reliance on technology in our daily lives could leave sensitive personal financial information more vulnerable to unwanted viewing or theft without proper safeguards in place," said Gavin Gee, director of the Department of Finance. "Our department is undertaking several initiatives to educate our examiners, the financial services industry, investors and consumers about the increased importance of cyber security."

In September 2014, the North American Securities Administrators Association (NASAA), of which Idaho is a member, reported that 62 percent of state-registered investment adviser firms participating in a NASAA pilot survey had undergone a cybersecurity risk assessment, and 77 percent had established policies and procedures related to technology or cybersecurity. "Investors are right to concern themselves with the safety of their financial information, and talk with their investment professionals about what steps firms are taking to safeguard client information," Gee said.

To help investors with that discussion, the department suggests asking the following questions:

- Has the firm addressed which cybersecurity threats and vulnerabilities may impact its business?
- Does the firm have written policies, procedures, or training programs in place regarding safeguarding client information?
- Does the firm maintain insurance coverage for cybersecurity?
- Has the firm engaged an outside consultant to provide cybersecurity services?
- Does the firm have confidentiality agreements with any third-party service providers with access to the firm's information technology systems?
- Has the firm ever experienced a cybersecurity incident where, directly or indirectly, theft, loss, unauthorized exposure, use of, or access to customer information occurred? If so, has the firm taken steps to close any gaps in its cybersecurity infrastructure?
- Does the firm use safeguards such as encryption, antivirus and anti-malware programs?
- Does the firm contact clients via email or other electronic messaging, and if so, does the firm use secure email and/or any procedures to authenticate client instructions received via email or electronic messaging, to work against the possibility of a client being impersonated?

"As a customer, you have the right to ask these questions and get answers as part of your due diligence and becoming an informed investor," Gee said.

\*\*\*\*\*

Investors can contact the Department at (208) 332-8004 or by visiting <http://finance.idaho.gov> for more information.