

# Investor Information Security Guidelines and Fraud Prevention

## Information Security is Everyone's Job

At Davidson, information security is very important. Our employees are fully aware of their responsibilities to keep your information safe, secure and confidential. We use the best technologies and practices to protect your information. However, there are some steps that you personally can take to help us keep your information secure.

### What can you do to improve your security?

While we do our utmost to ensure security and confidentiality, there are some steps that you can take to improve your security when using the Internet and when conducting business online. We invite you to explore this site to learn more about Internet security and protecting your identity.

**Anti-Virus Software.** You should have adequate anti-virus software installed on your computer. Anti-virus software attempts to identify, neutralize or eliminate malicious software (i.e. Virus, Trojan Horses, Root Kits, Malware, or Adware). The software should be updated on a regular basis.

**Firewalls.** Any computer or device connected to the Internet that is not properly protected is vulnerable to a variety of intrusions and attacks. A personal firewall will help protect you from intrusion. Firewalls create a barrier between your computer and the Internet. A firewall can be a hardware device, a software application or a combination of the two. Firewalls can prevent malicious attacks and block certain types of data from entering your computer.

### **Passwords.** Tips for Creating Unique Passwords:

- Never share your passwords with others.
- Create and use long passwords that consist of a mix of letters, numbers and special characters.
- Change your passwords frequently.
- Instead of a password, use a passphrase; which is sentence. (i.e. "Ilovemycat\$7")

**Test your computer for Security Vulnerabilities.** There are several tools currently available on the Web that you can use to test your computer system for security vulnerabilities. If your system is not configured properly, for example, it may be easier for hackers and intruders to break in. The following are tools you can try to evaluate your computer system.

<b>Tool</b>	<b>Publisher</b>
<u>FreeScan</u>	McAfee
<u>Shields UP</u>	Gibson Research Corporation
<u>Security Check</u>	Symantec

**Things you can do to protect your personal information:**

- Sign all credit cards as soon as they are received.
- Pay attention to billing cycles; if bills fail to arrive contact the company to ensure the bill has not been illicitly redirected.
- Review your financial statements and look for unauthorized transactions such as purchases and withdrawals.
- Limit the number of credit/charge cards owned to reduce exposure.
- If you have a lost or stolen card, notify your creditors immediately.
- Destroy cancelled checks and store new checks in a safe place.
- Destroy pre-approved credit card applications, credit card receipts, bankbooks, bank statements with checks and payroll statements (providing that they are no longer needed for tax purposes)
- Cancel all inactive credit cards.
- Review credit bureau files at least annually and immediately question any unknown credit inquiries or unauthorized accounts.
- Choose difficult passwords.

**Actions or practices to avoid:**

- Never record or keep a Client Card PIN, password or Social Insurance Number/Social Security Number in your wallet.
- Don't leave mail lying around and mail outgoing payments at secure U.S. Postal Mail boxes.
- Don't provide personal information such as birth date over the telephone and only provide your credit card number when you have initiated the call to a trusted third party.
- Don't leave your purse or wallet unattended at work, restaurants, health clubs, in a shopping cart or at social gatherings.
- Never lend credit cards to anyone.

**Phishing E-Mails & Websites.** “Phishing” Web sites may be used in conjunction with phishing e-mail scams to trick you into providing your personal financial information. Criminals will create a Web page or an email that appear similar to a legitimate thing.

## **What Davidson does to protect your information**

At Davidson, we use several layers of security to protect your information. We utilize technologies that keep your data secure while looking at your account over the internet. We employ the latest industry practices to ensure the integrity of our systems and the safety of your information. While we have taken a number of measures to ensure the security of your financial transactions and the confidentiality of your information, it is also important that you take precautions as well, to keep your information safe and secured.

**Secure Login.** For your protection, we require you to login to your Davidson on-line accounts using your username and password. Please contact your Financial Consultant if you need your password reset.

**More help from third-party resources.** Davidson is not affiliated with these third-party resources, and if you click on any of the below links, you will leave [www.davidsoncompanies.com](http://www.davidsoncompanies.com) and be taken to another site.

Federal Trade Commission: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

U.S. Department of Justice: [www.usdoj.gov/criminal/fraud/idtheft.html](http://www.usdoj.gov/criminal/fraud/idtheft.html)

OnGuardOnline.gov: <http://onguardonline.gov/phishing.html>