

# Online Security Fact Sheet

## What You Need to Know About Online Fraud

Online fraud has become big business and is highly sophisticated. These deceptive crimes are triggered using many forms and disguises:

- *email fraud*    • *spyware*
- *website fraud* • *browser hijacking*

These scams, viruses and malware are able to obtain login information and passwords through implanted keystroke loggers, which are used to steal confidential information in order to transfer money or commit other fraudulent activities.

## Safeguarding Your Information—Your Responsibilities

ViewPoint Bank is committed to providing you with information necessary to protect your business, financial information and assets. While we have many advanced security tools to protect your financial information, the most important security factor is YOU. **You are responsible for the security of your computer and networks.**

Please read over these important security safeguards. We strongly recommend the following actions to protect your computers and data.

### 1. Use Multi-Factor Authentication

Multi-factor Authentication (also known as Secondary Authentication) is a method of identifying a user by combining two or more types of information:

1. Something you know - User ID & Password
2. Something you have - Token and/or Digital Certificate

By using Multi-Factor Authentication, you are making it more difficult for someone to impersonate you on a system. ViewPoint Bank's current options for Multi-Factor Authentication are Security Tokens and Digital Certificates.

### ePoint Business Security Token (REQUIRED for initiating payments)



The Token is a small, portable device linked to your User ID that generates a new Personal Identification Number (PIN) every 30 seconds. Frequent PIN changes present a barrier to fraudsters. This industry best practice is:

- **Easy to use** – Tokens are only needed for the first transaction within a continuous session.
- **Easy to order** –You may order a token through secure messaging within ePoint Business or by contacting ViewPoint Bank Treasury Management Support at **972-801-5855**.

### Digital Certificate

Digital Certificates are electronic credentials stored on your PC that ensure that the computer accessing ePoint Business is an authorized PC.

## 2. Implement Dual Approval

Dual Approval requires a second user to approve funds transfers. We strongly recommend dual controls to perform Automated Clearing House (ACH) and wire transfers. This standard industry best practice is easy: One person initiates the payment; the other approves it and releases it for payment.

**Dual Approval used in conjunction with Multi-Factor Authentication has proven to be the highest form of protection against financial losses from online fraud.**

**Important:** If you choose not to implement these recommendations, your company and assets are at a greater risk for fraud. Because of this, a **signed waiver is required for any client who does not employ Dual Approval.**

Continued on back

### 3. Establish the following “Best Practice” Security Policies:

- Safeguard login credentials and **never share login credentials with others.**
- **Educate all users** on ViewPoint Bank security policies.
- **Monitor your accounts daily** for unexpected or suspicious activity.
- **Dedicate a PC or workstation** to be used only for your ePoint Business online transactions. Do not allow this dedicated computer to be used for other activities such as Internet searches, website browsing, accessing social networking sites or reviewing personal email.
- Access ViewPoint Bank ePoint Business through **our trusted Web address** available through the ePoint Business link at [www.viewpointbank.com](http://www.viewpointbank.com).
- **Use Anti-Virus software, Anti-Spyware and firewalls**, and check to ensure they’re updated regularly.
- Consult with your own **information systems security professionals** or engage third-party security consultants to ensure you are guarding against invasion by malware, viruses, Trojan horses, key logging software and other techniques used by hackers and fraudsters.
- **Be cautious about opening attachments**, downloading files from emails or using file sharing software regardless of who it’s from.

### 4. Use Additional Fraud Protection Services Offered by ViewPoint Bank

- Use **ACH Payment Authorization**, such as debit and credit blocks.
- Sign up for **ePoint email alerts** to instantly inform you when an electronic debit or credit hits your account.
- Use **repetitive payment templates** to prevent unauthorized modifications to key fields like beneficiary information.
- Set **payment limits** for all users authorized to initiate or approve funds transfers.

**Important:** ViewPoint Bank will never ask you to provide, update or verify your login credentials through email. This includes passwords, answers to authentication questions, or token PINs. In addition, ViewPoint Bank will never issue software downloads or upgrades through email.

### Additional Information

Remember, the security of your computer and networks is your responsibility. To learn more about safeguarding your financial information online, visit the following links on our website:

- [viewpointbank.com/ePoint Business](http://viewpointbank.com/ePoint Business) – available security tools and training
- [viewpointbank.com/home/resources/fraudsecurity](http://viewpointbank.com/home/resources/fraudsecurity) – additional security info

**If you suspect you may have been a victim of a fraudulent online banking scam regarding your ePoint Business account, contact:**

**Treasury Management  
972-801-5855**