

*Salisbury Bank is committed to helping your business and protecting your accounts. One way we do this is by keeping you informed about important news that affects your online security.*

## Fraud Protection Reminder for our Cash Management Customers

Recently, the media has reported that RSA, the makers of your Business e-Banking tokens, had experienced a cyber-attack that resulted in stolen information relating to the operation of the SecurID tokens.

Based on the details released by RSA, your data is not at risk. Any person who might attempt to use the stolen information to compromise your SecurID token would not succeed unless they also have your unique User IDs, passwords, answers to challenge questions and in some cases are also able to replicate your IP address. In order to mount a successful direct attack, someone would need to have possession of all this information.

Your tokens are still secure, especially when used as part of a layered security approach.

Salisbury Bank recommends the following important fraud prevention and protection strategies for keeping your Business e-Banking secure:

- Use best practices for online cash management services, including authentication for authorizing transactions online and/or dual confirmation of outbound transfers.
- Keep your SecurID token in a secure place.
- Keep your SecurID token serial number (located on the back of your token) secure. Once you enter your serial number to register your token, you should not have to re-enter the information.
- Utilize security features such as IP Restrict and Time Restrict. Call our Deposit Services Department at 860-435-9801 for more information or to enable these features.
- Review account activity periodically throughout the day and at wire/ACH deadlines to verify transactions.
- Immediately report any questionable transactions to Salisbury Bank by calling our Deposit Services Department at 860-435-9801.
- Reconcile accounts daily.
- Use best practices for computer security, including security of hardware, software and employee identity management. One of the best ways to protect your data and your accounts is to install anti-virus software, set up daily updates and schedule virus scans weekly.
- Warn employees against responding to emails or phone calls from the company's bank(s) requesting account or user ID information. Legitimate banks, including Salisbury Bank, have policies that prohibit the use of emails to request confidential or personal information.
- Create policies restricting employee use of business computers for personal use, including surfing the web for personal reasons, accessing personal email, browsing social networking sites, etc.
- Assign every user a unique User ID and password. User ID sharing should not be allowed.
- Require that online passwords be changed periodically. Best practices suggest at least every 90 days, more frequently if possible.
- Use "strong" passwords (alpha/numeric and special characters) that are not easily duplicated.
- Disable User IDs and password for employees on extended leave or vacation.

*This document is designed to provide informative material and is distributed with the understanding that it does not constitute legal or other professional advice. We suggest that you consult with your systems administrator, IT consultant, technical advisor or attorney with regard to your business' particular situation.*

### Salisbury Bank and Trust Company

5 Bissell Street  
Post Office Box 1868

Lakeville, Connecticut  
06039-1868

t: 860.435.9801  
t: 800.222.9801

[www.salisburybank.com](http://www.salisburybank.com)

© Salisbury Bank and Trust Company Member FDIC