

Best Practices for Protecting Online Payments and Financial Data Against Fraud

Salisbury Bank works to protect our customer and financial data and we take all security threats very seriously. We'd like to share some of the best practices we have learned to help you protect your business as well.

Although deploying appropriate anti-fraud technology is important, technology alone cannot protect your systems. Strong management controls are essential, and your people are your number one line of defense. Educate all your employees about Internet fraud and enlist them in your efforts to protect sensitive information.

General Fraud Awareness and Prevention

- ❑ Warn employees against responding to emails 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.
- ❑ Enforce employee security training as part of the new hire procedure, and conduct ongoing security awareness training to educate employees about online threats and the company's security policy.
- ❑ 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.
- ❑ Rotate banking duties among employees.

Online System Administration

- ❑ Assign dual system administrators for online cash management services.
- ❑ Assign every user a unique User ID and password. Do not share User IDs.
- ❑ Periodically evaluate employee job functions and remove online services that are no longer needed.
- ❑ Periodically review user settings to confirm that employees have access only to the functions needed for their jobs.
- ❑ 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 passwords for employees on extended leave or vacation.
- ❑ Delete User IDs and passwords as part of the exit procedure when employees leave the company.

Payment Initiation

- ❑ Segregate responsibilities among different employees for payments template maintenance, payments entry and payments approval.
- ❑ Establish different payment initiation and approval limits for employees based on their job level and responsibilities.
- ❑ Require dual approval to initiate wire transfers.
- ❑ Review account activity periodically throughout the day and at wire / ACH deadlines to ensure appropriate usage.

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. Opinions expressed herein are subject to change without notice. Information has been obtained from sources believed to be reliable, but its accuracy and interpretation are not guaranteed.

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

© Salisbury Bank and Trust Company Member FDIC