

Fraud and Liability: What You Need to Know

In today's high tech environment, businesses have to defend against various types of fraudulent schemes including wire fraud, business email compromise, malware and more.

Authorities are now warning business owners about an increase in altered checks. In some cases, an employee has mailed a check to a legitimate vendor only to find weeks later that the payment was never received. After investigating, it was discovered that the mail had been intercepted at some point between mailbox and recipient and the check altered to be made payable to a different payee than originally intended.

Protecting Your Account

The best way to protect your business and its finances is to view your accounts daily. While the balance may be accurate, it is best to verify that all checks were cashed by their intended recipient and that all transactions are legitimate. As a business, you must report any suspicious or fraudulent transactions **within one business day of the transaction date**. After that time, you may be held liable for any activity that posts to your account.

Convenient Tools For Account Monitoring

- ◆ **Account Alerts** - Customers who are enrolled in online banking may quickly and easily set up Real Time Account Alerts. You choose the type of notification you'd like: low balance amount, high balance, or any account activity at all. You can also choose whether to be notified by text or email.
- ◆ **My Mobile Money** - My Mobile Money allows you to set alerts and card restrictions based on transaction type, merchant type and location. You can even take action directly from the app, denying or approving charges in real time. Download the My Mobile Money app in the App Store or Google Play today!
- ◆ **Check Imaging** - Images of your cancelled checks appear in online banking shortly after they are processed. You can easily view the front and back of each check by clicking on its image when you access your online account, so you won't need to wait for your monthly statement to see your cancelled checks.

Business Newsletter

Issue 5 – Fall 2018

#TechTips for business owners



Mobile devices can create significant security challenges, especially if they contain confidential information or can access your business' network. It's best to require all users to protect their data using passwords and encryption.

Regularly back up your files to a cloud-based service, alternate location or external hard drive. In the event of a ransomware attack or a natural disaster, you will still have access to your most important information.



Educating your employees about the most recent scams and what preventative actions they can take is your number one defense against cyber crime. Sharing this newsletter with your staff is a great start!

**For more Tech Tips,
visit the Security page
at haverhillbank.com.**