

# Keeping Safe in CyberSpace

## Some Basics for Business and Their Customers

by  
Ray Abbott,  
SVP Cash Management  
WSFS Bank



**A**s many financial services professionals can attest to, Identity Theft is not a new issue, but one that is growing due to the rapidly expanding on-line facilities. We have indeed entered a brave new world of cyberspace, completing routine tasks today that we only would have dreamed about ten or fifteen years ago. In this digital environment, it is becoming a cat and mouse game between those who would protect their customers and institutions and the fraudsters who would steal from them...and the game is changing. Is your organization doing the right things to stop them? How about your customers? Are you educating them on the basic on-line security they need not only to protect themselves, but those with whom they do business? Creating an exhaustive list is nearly impossible, for new scams seem to appear faster than annoying pop-up messages, but here are some critical areas all those operating in cyberspace should be aware of.

### **Businesses Beware**

The caveat used to be “buyer beware,” but business, especially financial institutions need to be wary in today’s digital marketplace. When asked why he robbed banks, Depression-era criminal Willie Sutton replied: “because that’s where the money is!” In today’s challenging economy the same holds true, but the fraudsters don’t have to come in through the front door, they can do far more by slipping in with a simple Internet connection. Keyloggers, malware, phishing, pharming, viruses, etc... New terms come up every day. Cyber criminals are

targeting financial accounts of owners and employees of businesses across the world (and yes, Delaware) causing havoc and financial losses. Simply do a search on the Internet for “corporate account takeover” and view how many items come up. Consumer accounts are subject to Federal Reserve Regulation E which requires banks to provide reimbursement for certain losses. Regulation E does not apply to business accounts and therefore banks are not required to provide reimbursement for certain losses. This means businesses need to take a serious look at how they reconcile their accounts and do everything they can to protect themselves from a cyber attack.

Early on, cyber criminals mostly attacked large companies, but lately these have morphed into attacks on smaller companies, owners of the companies, and their employees’ accounts. Customers are coming to realize that corporate account takeover is a real threat. In October, 2010, the FBI announced that a cyber crime ring managed to steal \$70 million by targeting computers of medium-sized companies, towns and even churches. What can businesses operating on-line do to protect themselves? The most common strategy for deterring fraud has been to educate businesses about potential threats, as well as investing in technology to combat these threats. ACH Debt Block, Token Authentication, Multifactor Authentication, and Positive Pay, are just a few commercial banking products that have seen growth and are worth looking into, if you have not already done so.



### **If You Don't Control It, Who Will?**

Businesses actively engaged in on-line transactions should be proactive when it comes to exercising control over their transactions. Ignoring these areas of potential threat only affords opportunity to fraudsters. These include:

**ACH/Wire Authority Controls** – Providers need to employ strong risk mitigation controls over access, processing, submission and reconciliation of automated clearinghouse and wire operations. This includes using unique, dynamic and strong authentication mechanisms; requiring the separation of duties and dual controls over file and transaction creation, submission and verification/reconciliation. Online banking activities should be carried out from restricted function, stand alone or network segmented devices, hardened host without email and general web browsing compatibilities. Finally, activity notification and/or limit breached alerts should be established.

**Deposit/Transaction Account Controls** – To be sure of security, strong risk mitigation controls should be enacted over daily transaction activities and account reconciliation.

**General IT Controls** – Employ strong risk management controls throughout the Information Technology environment. In addition, while your IT people may be up on the latest trends, it doesn't mean your frontline

employees are. Periodic employee awareness training sessions should be conducted to keep all staff up to speed.

Another simple method is to have a dedicated computer only used for online banking. Often times this seems impractical for the small business, but it can be an effective strategy.

### **Other Best Practices for Business**

**Set up Alerts in Online Banking** - Customize alerts to automatically notify you when wire transfers are deposited into your accounts. Set up alerts to notify you of any ACH's, wires or book transfers coming out of your accounts.

**Reconcile Daily** - It is recommended that you reconcile your accounts daily. Strong account oversight is essential in today's ever changing technological environment.

**Understand the Administrator's Role** – Get a good understanding of the role of the System Administrator; they are solely responsible for allowing access to your business accounts. The System Administrator can create unlimited users and grant them access to appropriate accounts, and will also assign appropriate module access.

**Dual Control** - Dual Control allows one user to initiate a transaction but a second user to release it. Dual Control can be turned on for book transfers, ACH or Wire Transfers.

**Security Tokens** - Security Tokens are devices used to confirm the user's identity to the bank's system – often times, they are automatically required for ACH and Wire transfer modules by banks.

**Back up your files** – Finally, because no security method is completely foolproof. It's important to back up critical files regularly, before you get hit with a problem.

### **Your Customers – Your Security Partners**

Okay, your IT people are aware of the latest trends and threats and are doing all they can to protect you from within. You update your staff regularly to reduce internal risks. So, you're safe, right? Not necessarily. Are your customers cyber savvy to potential threats? A lax online customer can open up a wide range of potential threats not only to themselves, but to those with whom they do business...including their financial institution. Many instances of malware begin by clicking on an Internet link that asks for a response or action of clicking on a certain link. That's why computer safety should be stressed to your online customers through your website and in any way you interact with them...especially on line. Here are some simple common sense measures you should be sharing with your online customers:

- Always check the browser for a "lock" icon. It is important to understand that the lock signifies a secure communication channel to a website; however it does not indicate a legitimate website.
- Avoid accessing online banking or making purchases at wireless hot spots, Internet cafés and public Internet access points.
- Keep your firewall turned on. Your computer firewall acts as a security checkpoint that information must pass through before it can enter or leave your computer. Your firewall also helps to prevent software on your computer from accepting unauthorized updates or

*Continued on p. 18*

## Security

(continued from p. 17)

changes sent over the Internet.

- Keep your software up to date. Hackers are always looking to exploit weaknesses in software, and new security threats emerge every day. That's why you need to install updates provided by your software companies
- Use Antivirus Software. Antivirus programs scan everything that goes into your computer—including e-mail, discs, and data files—searching for thousands of known viruses. Keep your antivirus software current by subscribing to an antivirus service and automatically downloading the latest updates.
- Use Antispyware Software. Antispyware programs monitor your computer, looking for known spyware and watching for programs that try to install themselves without your knowledge or permission. When antispyware programs find something, they warn you and help you take action against the spyware. As with antivirus software, keep your antispyware software current, and automatically download the latest updates.

• Think Before You Click. Clicking the wrong link or attachment can expose your computer to spyware, a virus or ads that could clutter your screen and slow your computer. Be very cautious with attachments or links in e-mail or instant messages as well as social networking sites. If you know the sender, but the message looks suspicious, check before you proceed. If they didn't send the message, delete the e-mail or close the IM window. Never click Agree, OK, or I accept to get rid of a pop-up ad, an unexpected warning, or even an offer to remove spyware. Instead, close the window by clicking X in the upper-right corner.

• Download software only from websites you trust. File-sharing programs, and sites that offer "free" music, movies, games and other information are notorious for including unwanted software in downloads.

• Protect Your Passwords. Use a strong password—at least eight characters, with a combination of numbers, letters and symbols. Don't use the same password for banking that you use for other online accounts. Keep your password safe — Don't leave your password stored in a file on your computer or written on paper. Change your password often.

## Conclusion

Nothing is foolproof. As long as there are businesses and consumers operating honestly there will be criminals trying to rob, cheat, and steal from them. The current technological environment affords many opportunities for both. That is why it is incumbent upon financial institutions to educate their customers to be vigilant to stay on top of the latest trends and best practices for online commerce.



*Raymond Abbott is Senior Vice President and manager of WSFS Bank's Commercial Cash Management Services Department. Mr. Abbott has over 24 years of banking experience, the past 15 in Commercial Cash Management Services and Government Banking. In addition to his professional activities, Mr. Abbott is active in the local community serving on the Investment Committee of the United Way of Delaware and the Finance Committee of the United Way of Southeastern Pennsylvania. Mr. Abbott has a Masters in Business Administration from St. Joseph's University and a Bachelor of Arts degree from the University of Pittsburgh.*



## Building Bridges between the Financial Services Industry and Government



**A business-focused law firm with emphasis in the areas of...**

**Bank and Insurance Company Formation and Regulation**

**Government Relations**

**Environmental Regulation**

**Commercial Real Estate and Land Use**

**Corporate and Commercial Transactions**

**Civil Litigation**

Dover - (302) 678-3262  
email: pgs@pgslegal.com

Wilmington - (302) 654-3300  
www.pgslegal.com