ABA Insurance Services | SafeAlert®

March 2013 | Loss Control Advisory Bulletin from ABA Insurance Services

Recently, the media has reported hacker attacks on Apple, Facebook, Twitter and Microsoft (to name a few), which had the potential of accessing sensitive customer and company data considered valuable on the black market. Because of the ever-present potential of both identity and account theft through network or system breaches, the following frontline steps from the American Bankers Association should be shared with your customers.

Bank customers need to take an active role in protecting their privacy. Banks use a combination of safeguards to protect customer data, which allows them to detect unusual spending patterns and protect accounts. Customers also play an important role in safeguarding personal financial information.

To help ensure the safety of personal information, customers should follow these three tips:

- **Create c0mplic@t3d passwords.** Avoid birthdays, pet names and simple passwords like 12345. It is also important to change passwords at least three times a year. Because friendly theft – theft by someone the victim knows – is the most common type of identity theft or fraud, don't share your passwords with family members and be mindful of who has access to your personal information.
- **Continually monitor accounts.** Check account activity and online statements often, instead of waiting for the monthly statement. You are the first line of defense because you know right away if a transaction is fraudulent. If you notice unusual or unauthorized activity, notify your bank right away.
- **Protect yourself online.** Be sure computers and mobile devices are equipped with up-to-date anti-virus and malware protection. Never give out your personal financial information in response to an unsolicited email, no matter how official it may seem. Your bank will never contact you by email asking for your password, PIN, or account information. Only open links and attachments from trusted sources. When submitting financial information on a website, look for the padlock or key icon at the top or bottom of your browser, and make sure the Internet address begins with "https." This signals that your information is secure during transmission.

If your customer is a victim of fraud and suspects that their personal information has been compromised, the following steps should be taken by your customer:

- Call your bank and credit card issuers immediately so necessary steps can be taken to protect accounts.
- A police report should be filed and the fraud units of the three credit-reporting companies should be contacted.
- A "victim statement" should be placed in credit reports.
- Make sure to maintain a log of all the contacts you make with authorities regarding the matter. Write down names, titles, and phone numbers in case you need to re-contact them or refer to them in future correspondence.
- For more advice, contact the FTC's ID Theft Consumer Response Center at 1-877-ID THEFT (1-877-438-4338) or www.ftc.gov/idtheft.

Additional resources to educate and inform your customers of safe banking habits can be obtained at aba.com/Consumers.