

IN THIS ISSUE:

- ≡ **NEW!** Fraudulent Canadian Check Coverage Available
- ≡ For the Holiday Season: The Latest on Phishing
- ≡ Meet Patricia Williams, New Senior Account Executive

NEW! Fraudulent Canadian Check Coverage Now Offered.

ABA Insurance Services introduces a NEW Foreign Check Rider that extends Bond coverage for fraudulent Canadian checks.

Typically, losses due to fraudulent Canadian checks are not covered under the Financial Institution Bond because such losses are precluded by Exclusion (o) which operates to bar coverage when domestic banks honor fraudulent checks drawn on financial institutions outside of the United States.

Where domestic banks are subject to the Uniform Commercial Code's (UCC's) "Midnight Deadline" as well as Federal Reserve Rule CC, which limit the amount of time a bank has to revoke settlement, foreign banks—including Canadian banks—are not subject to the UCC or the Federal Reserve's rules. Instead, Canadian banks' right to revoke settlement may be as long as one year from the date that the item is discovered as fraudulent, regardless of when the fraud is discovered. Because the discovery period can be indefinite, an item drawn on a foreign bank is never finally paid like domestic items; therefore, foreign checks are unavoidably subject to Exclusion (o).

The Foreign Check Rider from ABA Insurance Services remedies this issue by modifying Exclusion (o) under the Bond to include coverage for forged or altered checks drawn upon Canadian financial institutions.

For more information, call or have your agent call ABA Insurance Services at 800-274-5222 or visit abais.com.

[Article continued on next page ⇨](#)

Reloading your Tackle Box for the Holiday Season: The Latest on Phishing.

by Brian Schaeffer, CISSP, CISA and columnist for NetDiligence® eRisk Hub® portal, www.eriskhub.com

We've been battling phishing for the better part of 15 years. It is one of the most effective means of compromising a person's or company's accounts. In the early days, due to the use of broken English, it was relatively easy to spot a phishing attempt to steal information. Now, however, phishing techniques have evolved and with the adoption of social media and mobile technologies, these threats have become increasingly difficult to recognize and combat.

As we've learned over the years, phishing is a method of obtaining personal information by some form of social engineering.

[Article continued on next page ⇨](#)

SIDE NOTES

ABA helps banks with fraud prevention and security

Because fraud is a continuing issue for banks, the ABA offers an array of resources to help prevent, measure, report and prosecute fraud. Materials and surveys are available to help banks understand the fraud experiences of other banks in order to assess their own bank's risk. These resources can be accessed through aba.com/Solutions/Fraud.htm. Some are exclusive to ABA member institutions only, such as the Bank Risk News, a monthly summary of useful information, tips and case studies regarding matters of bank security. If your bank is already an ABA member, you can sign up for the Bank Risk News e-bulletin by going to aba.com/Members+Only/bulletin.htm and registering a password. If your bank isn't a member and would like to learn how to join, contact ABA's Karen Call at 202-663-5585.

Also available on aba.com is the recently launched ABA Bank Capture Program, a data sharing platform for banks to report, share and analyze their robbery and other bank crime data. To enroll, contact ABA's Doug Johnson at 202-663-5059.

Meet our new Senior Account Executive, Patricia Williams, CPCU



We are pleased to announce that Patricia Williams has joined ABA Insurance Services as a Senior Account Executive. With a total of 24 years in the insurance industry, Pat was formerly with Zurich for 14 years, first as a Financial Services Executive and then as a Regional Practice Leader for the Northeast and MidAtlantic regions. Previously, she was with Kemper Insurance and Aetna Casualty & Surety. Pat graduated from Towson University with a BS in Mass Communications.

Responsible for new business development in Delaware, Maryland and Virginia, and accounts of \$1 Billion and more in assets, Pat can be reached at 800-274-5222, ext. 1280 or pwilliams@abais.com.

■ Reloading your tackle box for the holiday season: The latest on phishing, continued from page 1

Phishers attempt to convince people to click on a link or disclose personal information by tricking them into thinking they are doing something necessary and legitimate. These days phishing takes many forms. Here are a few of the latest types of phishing:

- ≡ **Spear Phishing** is the most popular technique targeting a specific group. Spear Phishing attempts are more sophisticated, using targeted and relevant details to trick the victim. Most of the breaches that occurred this year started with this method.
- ≡ **Whaling** is phishing aimed at senior management or other high-value targets of an organization.
- ≡ **Smishing** uses SMS or text messages sent to mobile devices as the medium for the phishing attack.
- ≡ **Vishing** uses voice communications as the means of attack. These attacks can use Voice over IP (VoIP) and/or spoofed Caller-ID to aid in the scam.
- ≡ **Tabnabbing** opens new browser tabs that look similar to sites that were already open. These tabs quietly redirect the victim to a phishing site behind the scenes. Many users don't notice the change and click or login to the phishing site.
- ≡ **Evil twin** creates a fake wireless hotspot and collects personal data from everyone who connects to it. This type of phishing attack is popular in airports, hotels, coffee shops, etc.

Holidays Bring Out the Bad Guys

The holiday season typically sees an increased number of phishing attacks. Rohyt Belani, CEO of PhishMe, has identified a few popular holiday phishing attacks. These attacks start with one of the following phrases:

- ≡ Kick off your holiday shopping with this 10% off coupon for any store at [your local mall].
- ≡ [Your company] thanks you for your hard work this year and invites you to enter our holiday raffle.
- ≡ A year-end inspection has turned up mold in offices in our building at [your work address].
- ≡ [Your company] is migrating its payroll system before the end of the year. Please enter your updated information to avoid interruption of your direct deposit.

An Even Bigger Challenge for Financial Institutions

According to Checkpoint, the vast majority of phishing attacks are aimed at the payment and financial industries. Financial institutions have a dual responsibility to protect their organizations and raise awareness within their largely non-tech savvy customer bases.

Ongoing customer education is the most effective way of defusing phishing threats. When communicating with customers, the key points to stress are:

- ≡ Never click on a link contained in an email from your financial institution. Take the time to type the URL into the browser. You can hover your mouse over the URL, without clicking, to see where it will take you.
- ≡ Financial institutions don't ask for personal, password or credit card information in an email. If you receive an email that requests this type of information, call the institution to confirm the request.
- ≡ Any message starting with "Dear Customer" instead of your name is clearly suspect.

As the phishing landscape continues to evolve, it is critical that financial institutions keep informed on current attacks and communicate regularly with their customers. Above all, banks must educate customers to "Trust but verify."

About the Author

Brian Schaeffer, Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA), is a columnist for the NetDiligence® eRisk Hub®, portal, www.eriskhub.com. With 17+ years experience in banking, and information security and technology, Brian is often cited as an authority in banking publications and local media. In November of 2010, he was named one of the New Leaders in Banking by the New Jersey Bankers Association. Brian has given briefings to the FBI on wire fraud, check fraud, and other information security topics. He currently serves as President of the Philadelphia chapter of Infragard and has worked on various cyber-defense initiatives with the FBI and the Department of Defense.

For more loss control information or to view this SafeTalk newsletter online, visit abais.com. To subscribe to SafeTalk®, request reprints, or if you have additional questions about this newsletter or its articles, please contact us at marketing@abais.com or 1-800-274-5222.

ABA Insurance Services Inc. dba Cabins Insurance Services in CA, ABA Insurance Services of Kentucky Inc. in KY, and ABA Insurance Agency Inc. in MI.
The Foreign Check Rider is not available in all states currently. Please check with ABA Insurance Services regarding availability.