2017 ABA Issue Summary

Phishing

Contact: Sarah Grano, ABA Public Relations (202) 663-5470 or sgrano@aba.com

More bank customers rely on the internet to do their banking than ever before and cybercriminals are taking advantage of that trend.

- While online banking and e-commerce are very safe, you should always be careful about giving out your personal financial information over the internet.
- Consumer education is a powerful weapon in the fight against phishing. Most banks have anti-phishing tips on their websites or have mailed fraud prevention tips in their monthly statements.
- Protecting your money is a partnership between you and your bank. The more precautions we all take, the safer your money – and your information – will be.

Phishing is a type of online scam that has increased in both number and sophistication.

- Phishing attacks occur when criminals use "spoofed" emails and fake websites of trusted companies to coerce consumers into sharing account information.
- According to the Anti-Phishing Working Group, the financial services industry remains one of the most targeted industries for phishing scams.
- The Anti-Phishing Working Group documented 789,068 unique phishing sites in 2015, up from 614,178 in 2014, with financial services being the most targeted industry.[1]

Banks combat phishing schemes by educating their employees and customers, installing fraud detection software and working with industry coalitions.

- Banks have software – such as "neural network" technology – that can detect unusual spending patterns and alert bank employees, who can contact the customer and re-secure a compromised account.
- Banks work closely with industry coalitions, such as the Anti-Phishing Working Group (www.antiphishing.org), to team up against criminals. These groups help identify new schemes and develop counter-phishing methods.

Consumer Tips:

- **Don't click on suspicious links or attachments.** Visiting unsafe, suspicious or fake websites can lead to the intrusion of malware. Be cautious when opening e-mails or attachments you don't recognize even if the message comes from someone in your contact list.
- **Never give out your personal financial information** in response to an *unsolicited* phone call, fax or email, no matter how official it may seem.
- **Do not respond to email that may warn of dire consequences if you do not validate your information immediately.** Contact the company to confirm the email's validity using a telephone number or website you know to be genuine. Clicking on a link could give a criminal access to your personal information.
- **Check your credit card and bank account statements regularly** and look for unauthorized transactions, even small ones. Report discrepancies

Phishing

(continued)

immediately.

- **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 web address begins with "https." This signals that your information is secure during transmission.

- **Report suspicious activity** to the Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center at www.ic3.gov.

- **If you believe you have responded to a spoofed email**, **contact your bank immediately** so they can protect your account and your identity. For information on identity theft, visit ABA's consumer page on identity theft and see additional resources on phishing.

Background
Phishing attacks use “spoofed” e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, Social Security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince recipients to respond to them.

Sources:

[1]*Phishing Attack Trends Report*, Anti-Phishing Working Group. Retrieved from www.antiphishing.org