

From: Frank Keating and Rob Nichols [<mailto:keating@aba.com>]
Sent: Thursday, October 01, 2015 5:02 PM
To: Charlotte Birch <CBirch@aba.com>
Subject: Security alert regarding aba.com

TO: ABA Shopping Cart Users

FR: Frank Keating, ABA President and CEO
Rob Nichols, Incoming ABA President and CEO

Like the banks we serve, ABA takes data security very seriously. We also recognize that despite significant security measures, breaches can and do occur. We are writing today to alert you to such a breach.

ABA has learned that email addresses and passwords used to make purchases or register for events through aba.com's Shopping Cart have been compromised. Though we are not aware of any fraudulent activity associated with this, we are taking the breach seriously and have launched an immediate investigation. This memo is to let you know what we know, and what you can and should do to protect your information.

What we know so far

At least 6,400 records composed of ABA Shopping Cart user names and passwords were posted online. We have seen no evidence that the hacker has also accessed credit card or other personal financial information but will advise you immediately if we learn otherwise.

What you should do

We have taken the precaution of resetting your Shopping Cart password and ask that you log in now to establish a new one. To do so, please follow these instructions:

- Go to ABA's website by typing "www.aba.com" in your browser.
- Click on the Shopping Cart icon in the top right corner.
- If you know your user name, click on the "Forgot your password" link and follow the instructions.
- If you do not remember your user name, email shoppingcartinquiries@aba.com or call 1-800-BANKERS (226-5377).

If you use the same password to access other sites -- for example, Amazon, airlines or other shopping sites -- we strongly recommend you change those passwords as well. We also request that you do not recycle passwords that you have previously used.

As always, please also be on guard against phishing scams and refrain from clicking on links in suspicious emails.

What's next

ABA is working with a cybersecurity forensics company to identify the origin and full extent of this breach. We also continue to work with cyber information-sharing groups such as FS-ISAC to identify threats, spot breaches and respond quickly. We will keep you apprised of this investigation and what we learn. In the meantime, please accept our apologies for any inconvenience this has caused.

If you have any questions, please contact ABA Member Services at 1-800-BANKERS (226-5377) or visit aba.com/alert.

