***NOTICE****: The following has been provided by WBA committee and section volunteers for use by member banks.
It should be reviewed and revised as appropriate to the user-bank’s own policies, procedures, and practices.*

**ATM Fraud: Six Tips to Reduce the Incidents**

ATM fraud is very prevalent in the United States at this time. The two most common methods are either skimming devices attached to ATM’s and gas pumps or by compromising the card PIN. It is important that we as card users should pay attention to the way we use our cards.

Here are six tips that will help to protect us from these frauds:

1. Be wary of anything about the ATM machine that looks out of the ordinary, such as odd-looking equipment or wires attached to the device.
2. Look for a "no tampering" sign. Crooks often place these to stop anyone curious about a new piece of equipment.
3. Steer clear of a jammed ATM machine that forces customers to use another ATM that has a skimmer attached. Often, the criminal will disable other ATMs in the area to draw users to the one that has the skimming device on it.
4. Customers should check their bank accounts regularly to make sure there are no unusual or unauthorized transactions. Federal law limits loss from ATM fraud, and many banks offer additional protection. Consumers should check with their financial institution for details.
5. If you see anything unusual or suspicious around an ATM, or if you find unauthorized ATM transactions on your bank account, immediately notify local law enforcement, as well as your financial institution and/or the establishment where the ATM is located.
6. Always protect your PIN: Don't give the number to anyone, and cover the keypad while you are entering your PIN.

An extra basic tip is to never write your PIN on your card. Even now, that remains a common mistake made by many people.