

Maryland Nonprofits FAQ

Your nonprofit questions answered.

Q: HOW CAN I WORK TO KEEP UP WITH GOOD INTERNAL CONTROLS WHEN BANKING ONLINE?

A: There are many benefits associated with incorporating online banking into your financial efforts. However, with the ease and cost savings online banking affords, there is also the opportunity for impropriety in the midst of online banking.

Any nonprofit that is engaged in online banking should be sure to have a comprehensive, well defined policy for ensuring that proper controls are in place. Any policy requires tailoring to the services available online and the requirements of the particular bank.

For instance, the policy should provide safeguards that only authorized personnel actually have access to the online banking processes.

Methods of identifying authorized users may include the following:

- **Who you are:** such as fingerprints or iris scans is the most secure because it cannot be shared or stolen but is costly and rarely used for banking operations;
- **What you know:** which includes user names and passwords, is the most commonly used online;
- **What you have:** such as an access card or key. Banks will sometimes issue a "token" device which generates random numbers every 30 seconds or so. For certain transactions such as outgoing wire transfers, the user must enter the current number on the token in order to complete the transaction. The token has an external serial number which is linked to a particular user's access code.

One of the biggest concerns is that an unauthorized user will learn what you know (passwords, user names) and/or obtain what you have (token or device) and create a security breach. As such your online banking policy should strongly note that user identifications and passwords are not to be shared with anyone at any time. Likewise, when tokens or access cards are used, the user must be held responsible for the security of each token.

The policy should specify who (by position or title) is authorized to add/edit users of the online system. As such, the financial institution may have various levels of privileges granted to individuals with access to the account. For instance, some users may only be able to view transactions or balances. Others may be able to view and print transactions or balances.

The policy should specifically define whether each authorized user may initiate vendor payments and the dollar limit, and which users may approve vendor payments and dollar limit and who may update the approved vendor list. *[Initiation of payments is telling the system whom to pay, when to pay, and the dollar amount. Approval is required before the payments are actually transmitted. The same individual may have privileges to initiate and approve payments or it may be a two person process.] Organizations may establish a pre-authorized list of payees/vendors that can be updated as needed.*

The policy should also address fund transfers. The policy should state who is authorized to initiate and/or approve transfers between accounts owned by the company with dollar limits (or unlimited).

The policy should also indicate who is authorized to initiate and/or approve outgoing wire transfers or ACH (Automated Clearing House) transactions with dollar limits.

The policy should address who can initiate and/or approve a stop-payment order.

The policy should also outline responsibility for review of monthly bank statements by individuals not directly responsible for the online banking processes.

August 2009