

Information security



**James W.
"Jim" Yates**

The security of our membership's personal information is a very high priority for all of us at the MBA. We have all become aware of major corporations, banks, and even state and federal government systems that have been attacked by hackers. As a result of these attacks, the sensitive and personal information of millions of Americans has been compromised.

Cybersecurity is among the most significant challenges for all business organizations, including the MBA. As such, we have implemented an information security program based on a model law drafted by the National Association of Insurance Commissioners (NAIC), as well as on our own operations.

NAIC drafted this model law after almost two years of extensive deliberations and input from state insurance regulators and representatives for consumers and the insurance industry. While NAIC drafted the model, it is up to each individual state whether to adopt the law as is, modified to fit their needs or not at all.

To date, eight states have adopted some form of the model law (South Carolina, Ohio, Michigan, Mississippi, Alabama, Delaware, Connecticut and New Hampshire). Legislation to enact a version of the model law has been introduced in other states such as Nevada and Rhode Island.

Within MBA's information security program, we monitor and manage material risks, perform vendor and third-party oversight, have third-party intrusion tests performed, and can report on any security incidents and breaches. A portion of the monitoring of our intrusion prevention capabilities is automated and reported by our software and hardware systems. We continually strive to protect our membership and to maximize the capabilities of our system to stay ahead of attempts to compromise our data.

In addition to protecting our members' information on our computer systems from cyber attacks, we also take numerous steps to ensure that their information is secure, no matter the format.

When members call MBA or MBA calls members regarding a policy, they will be asked several questions to determine if they are the policy owner. They will be asked to verify their Social Security number, date of birth and address. MBA will speak only to the policy owner regarding the details of a policy, unless we have received permission from the owner of the policy to speak to someone else.

Whenever a conversation regarding a policy takes place, whether initiated by MBA or the member, notes are taken.

These notes then are added to the policy file in our database for future reference. We also maintain hard copies of our members' policy files. All hard copies of policy files and members' information are housed in a secured area.

Additionally, all policy documents are electronically imaged and stored in our database; thus, they always are available should the hard copies be destroyed in the event of a disaster. Furthermore, the database is encrypted and backed up off site. The database, and its backup, can be accessed only by MBA from our office or our disaster recovery location if necessary.

Any time there is a request to withdraw funds from or cancel an annuity policy, the policy owner's signature is verified. This is taken a step further when a life insurance policy is canceled. In this case, the policy owner's signature must either be notarized or the member's signature must be verified by a branch officer.

MBA requires written and signed requests to add, or make changes to, a policy's beneficiary or to change the member's address of record. Any addition or changes to a beneficiary are processed immediately upon receipt at MBA to ensure that any benefit claims are paid to the proper individual per the policy owner's request.

MBA has policies in place to ensure that any communication via email that includes a member's private information is sent in an encrypted format. Additional policies are in place governing cell phone usage in the work area that contains our members' sensitive information.

Protecting our members' money is as important to us as protecting their private information. Statements are mailed to the policy owners to confirm cash values, dividend amounts and loan values. Policy owners should contact MBA immediately if they notice any discrepancies.

It is our goal to process all premium payments received in our office on the day received. Any payment that is not processed on the day received is secured in our safe until the next business day. Once these checks and money orders are processed, they are secured for an additional 90 days. After 90 days, the checks and money orders are shredded. This process fully complies with banking regulations.

In addition to shredding any checks and money orders received at our office, MBA also shreds any discarded documents that contains our members' information. These documents are kept under lock and key until shredding is completed by a shredding and records management company contracted by MBA.

Members who receive monthly annuity payments are required to provide "proof of life" annually by having their signatures notarized on our proof-of-life letters. This ensures that our members are the individuals receiving the payments.