alloya℠
Corporate Federal Credit Union

Part 717-Subpart J-Identity Theft Red Flags of NCUA's Rules and Regulations requires all federal credit unions that offer or maintain one or more "covered accounts" to develop and maintain an Identity Theft Prevention Program.

Section 717.90(b)(1) of NCUA's Rules and Regulations defines an "account" as:

> "a continuing relationship established by a ***person*** [emphasis added] with a federal credit union to obtain a product or service for personal, family, household or business purposes."

Section 717.90(b)(3) of NCUA's Rules and Regulations defines a "covered account" as:

> "(i) an ***account*** [emphasis added] that a federal credit union offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, checking account, or share account; and
>
> (ii) any other ***account*** [emphasis added] that the federal credit union offers or maintains for which there is a reasonably foreseeable risk to members or to the safety and soundness of the federal credit union from identity theft."

While this rule is directed towards consumer related accounts, Alloya Corporate FCU acknowledges there is no exemption for corporate credit unions. That said, Alloya does not offer or maintain accounts to individual consumers and as such does not offer or maintain covered accounts as defined in the regulation.

However Alloya recognizes the importance of maintaining the privacy of its member credit unions and their members as well as the confidentiality and security of all personal, corporate and financial information it comes in contact with when performing services for your credit union. Alloya is keenly aware of the severity of identity theft in today's society and considers identity theft a serious threat. To this avail, Alloya has and maintains a comprehensive Information Security Program as well as a Privacy and Information Protection Policy.

Alloya's Information Security Program requires, among other things:

- A Board approved Information Security Policy and associated internal processes;
- Regular management reports;
- Monthly external and quarterly internal vulnerability assessments;
- A secure electronic product delivery channel;
- An advanced firewall solution,
- A robust intrusion detection system;
- Multiple anti-virus scanning engines;
- Automated Windows patch management; and
- Automated security monitoring and alerting.

Alloya's Privacy and Information Protection Policy underscores Alloya's commitment to proper information management and handling practices. This policy addresses, among other things:

- The collection of non-public consumer information;
- The disclosure of confidential information to non-affiliated entities;
- The prevention of identity theft;
- Identity Theft Red Flags;
- An acceptable usage statement; and
- Alloya's publicly accessed websites and data servers.

Section 717.90(c) of NCUA's Rules and Regulations states:

> "each federal credit union must periodically determine whether it offers or maintains covered accounts."

Within the "Identity Theft Red Flags" section of the Privacy and Information Protection Policy, Alloya indicates it will re-assess its accounts on at least an annual basis to determine whether it is offering or maintaining covered accounts.

All of these aspects, combined with qualified staff and regular training for all employees, results in an environment in which privacy and information security are thought of in every aspect of Alloya's business.