GEORGIA CREDIT UNION Affiliates
6705 Sugarloaf Parkway, Suite 200
Duluth, GA 30097
(770) 476-9625 • (800) 768-4282
AMERICA'S CREDIT UNIONS

September 18, 2006

Mary Rupp
Secretary of the Board,
National Credit Union Administration
1775 Duke Street
Alexandria, Virginia 22314–3428

Re: Proposed Rule 717 – Identity Theft Red-Flags

Dear Ms. Rupp,

The Georgia Credit Union League (GCUL) appreciates the opportunity to comment on the proposed guidelines that identify "red flags," which are patterns, practices, or activities that indicate the possible risk of identity theft, along with proposed rules requiring financial institutions and other creditors to implement the guidelines. GCUL is the state trade association and one member of the network of state leagues that make up the Credit Union National Association (CUNA). GCUL serves approximately 188 credit unions that have over 1.7 million members. This letter reflects the views of our Regulatory Response Committee, which has been appointed by the GCUL Board to provide input into proposed regulations such as this.

Background:

The FACT Act was enacted in December 2003 and includes a number of provisions that address the detection and prevention of identity theft. These include a requirement that the appropriate regulatory agencies (Agencies) issue guidelines for financial institutions and other creditors with regard to identity theft. These guidelines must identify patterns, practices, and specific activities that indicate the possible existence of identity theft.

The FACT Act also requires the Agencies to issue rules requiring financial institutions and other creditors to establish policies and procedures for implementing the guidelines that identify possible risks to consumers or risks to the safety and soundness of the institution. The rules must also require credit and debit card issuers to assess the validity of change of address requests when there is also a request for an additional or replacement card, which is often an indication of identity theft.

As required, the Agencies have proposed guidelines that identify patterns, practices, and specific forms of activity that indicate a possible risk of identity theft (referred to as "Red Flag Guidelines"). The Agencies have also proposed rules requiring each financial institution to implement a written Identity Theft Prevention Program, which must contain reasonable policies and procedures that address the risk of identity theft. These rules also require financial institutions to incorporate relevant indicators of identity theft into their programs from among those outlined in the Red Flag Guidelines. The Agencies have also proposed rules to require credit card issuers to implement the reasonable policies and procedures to address the validity of a change of address, as well as rules that provide guidance on policies and procedures that a user of credit reports should use if it receives a notice of address discrepancy from one of the nationwide credit bureaus.

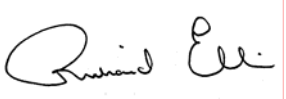
Summary of GCUL's Position:

- "Red flags" are generally defined as patterns, practices, or activities that indicate the possible risk of identity theft. This would include situations in which there is a "possible" risk of identity theft, even though the existence of identity theft is not necessarily indicated. An example would be the receipt of a "phishing" e-mail or a security breach. We believe this definition to be too broad and are concerned how this could be applied in certain cases. For example, the mere fact a member receives a phishing email doesn't, by itself, constitute a red flag. However, if a member were to respond to this type of email, then appropriate steps should be taken.
- We believe the requirement that the financial institution's program must incorporate relevant "red flags" from: 1) the Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation that is incorporated as an appendix to the proposed rules; 2) any applicable supervisory guidance, either now or in the future; 3) incidents of identity theft that the institution has experienced; and 4) methods of identity theft that the institution has identified that reflect changes in identity theft risks to be sufficient sources for a list of red flags. However, we encourage that all red flags not be mandated and stress that each institution be able to determine it's own applicable standards.
- The requirement that a financial institution using a third party's computer-based program to detect identity theft to independently assess whether the program meets the requirements of these rules and not rely on the representations of the third party is overly burdensome and one that will likely increase costs substantially, especially for smaller institutions lacking the staffing and expertise necessary to make this assessment. Smaller institutions would likely have to outsource this assessment, further increasing costs for compliance. Since each institution is responsible for compliance under the rules, it is not necessary to incorporate the standards by which they can comply. We believe this provision should be eliminated. In many instances, a third party solution has proven to be more stringent than required.

- We believe the list of “red flags” provided in the proposed guidelines to be specific enough. While it is a lengthy list, numerous examples are helpful to smaller institutions that do not have dedicated experts in this field.
- One of the “red-flags” listed is when an account is being used after being inactive for a long time. The FACT Act indicates that the account should be inactive for two years before it should be considered a concern. We believe this time period should be removed because different account types are used in different ways, which may affect the frequency of usage.
- Under the proposal, when required to determine the validity of a request for an additional or replacement credit or debit card shortly after receiving a change of address request, the card issuer must either:1) notify the cardholder of the request at the cardholder’s former address and provide the cardholder with a means to promptly report an incorrect address; 2) notify the cardholder of the address change request by another means of communication previously agreed to by the issuer and cardholder; or 3) use other means of evaluating the validity of the address change. We would suggest further elaboration on item number three to include additional examples. The implementation of this practice will also increase costs to all institutions.
- Many of the regulatory requirements under this proposal are duplicative of those required under the Customer Identification Program (CIP), which is required under the USA PATRIOT Act. We would encourage the Agencies to eliminate the redundant parts of this proposal in order to streamline compliance efforts.

Thank you for the opportunity to comment on the proposed guidelines that identify “red flags,” which are patterns, practices, or activities that indicate the possible risk of identity theft. If you have questions about our comments, please contact Cynthia Connelly or me at (770) 476-9625.

Respectfully submitted,



Richard Ellis
Vice President/Credit Union Development
Georgia Credit Union League