Cooperative Credit Union Association
Data Breach Principles

Objective:
The Association is in favor of strong national data security and consumer notification standards with effective enforcement provisions. Any new data protection law should address both privacy and data security. This legislation should be applicable to any party who collects, uses, shares, or has access to important consumer financial information.

New standards
- The focus of federal data security legislation should be on the subjects of reimbursement, consumer notification, and stricter data security standards focused on the prevention of theft and misuse
- Model standards for retailers should mirror existing federal law governing financial institutions such as the Gramm-Leach Bliley Act ("GLBA") relative to notices and data security

Reimbursement
- The costs of a data breach should be borne by the entity responsible for the breach
- Credit unions currently bear a disproportionate burden in covering the costs of breaches that occur beyond their domain. In the situation where a credit union reissues credit or debit cards due to such a breach, those costs must be reimbursed in the form of a fixed dollar amount
- A federal agency with security compliance examination authority over merchants should be identified and should also possess the authority to determine reimbursement levels

Notification
- Credit unions should be able to inform their members about the breach, including the entity at which the breach occurred
- The breaching party should provide notification as expediently as possible but no later than 30 days from discovery
- Any flexibility in this timeframe must relate to an ongoing law enforcement investigation or other appropriate intervening activity

Right of Action
- A law should provide mechanisms to address the harms that result from privacy violations and security violations, including a right of action

Qualified Preemption
- Qualified federal preemption is recommended. Federal law governs except in the event of a conflict between individual state and federal legislation
- Enforcement authority should be permitted for individual states

Safe Harbor
- Credit unions are subject to strict data protection and notification standards under GLBA, and are also heavily regulated and subject to regular supervisory examinations. To relieve additional regulatory burden, credit unions seek safe harbor protections within any uniform federal data security standards, such as a provision that compliance with GLBA provisions is deemed compliance with similar federal data breach standards