

Cooperative Credit Union Association Data Breach Principles

The Association is in favor of strong national data protection and consumer notification standards with effective enforcement provisions. This legislation should be applicable to any party with access to important consumer financial information.

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
- Notification should be provided 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

New standards

- The focus of proposed federal legislation should be centered on the subjects of reimbursement, consumer notification, and stricter data security standards for retailers
- Model standards for retailers should mirror existing federal law governing financial institutions such as the Gramm-Leach Bliley Act (“GLB”) relative to notices and data security

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 GLB, 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 GLB provisions is deemed compliance with similar federal data breach standards