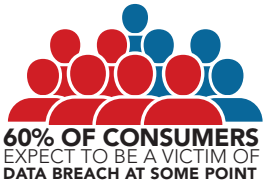
Merchant Data Breaches

Consumer data is at considerable risk because merchants do not have to follow strong data security requirements like credit unions. All who hold personal data should be subject to strong federal security requirements.

Credit unions cover the costs of fraud, blocking transactions, reissuing cards, increasing staffing at call centers and monitoring consumer accounts, but no one compensates the consumers for harm from the information that is lost. Merchants have been vulnerable to large and small data breaches, which cost credit unions and their members significantly and enrich criminal and other cyberterrorists.



- Nearly 60% of consumers expect to be a victim of data breach at some point.
- In 2017, 1,579 data breaches occurred in the U.S., a 44% increase from 2016.

Data breaches continue to be a problem, even when they are not in the news cycle. The number of compromised records jumped 389% in 2017 to a total of nearly 180 million records.

Financial institutions are subject to strict data security standards under the Gramm Leach Bliley Act (GLBA). Retailers are not.

- Merchant data breaches have compromised millions of American consumers' personal financial information, causing them to be at risk for identity theft and other fraud.
- More breaches occurred in 2017 by the business community than breaches in the healthcare industry and government combined.
- Business breaches accounted for 55% of total breaches and 91% of compromised breach records in 2017. In contrast, banking/credit/financial firms (including credit unions), accounted for 8.5% of breaches and 1.7% of compromised breach records.

Congress should pass legislation that would impose data security standards on merchants to protect consumers and reduce criminal access to financial information.

Source: ITRC (Identity Theft Resource Center)

To be protected, American consumers need:

Strong National Data Protection
and consumer notification standards with effective enforcement provisions are needed to ensure sensitive data is protected.

Recognition of Robust Data Protection
and notification standards that credit unions and banks are already subject to.

Preemption of Inconsistent State Laws
and regulations in favor of strong Federal data protection and notification standards.

Ability for Credit Unions and Banks to Inform
customers and members about a breach, including where it occurred.

Shared Responsibility
for all those involved in the payments system for protecting consumer data. The costs of a data breach should ultimately be borne by the entity that incurs the breach.