LIBERTYID® BUSINESS SOLUTIONS

Cyber Security Regulatory Requirements to Keep Consumer Information Safe

- Companies need to designate a "Qualified Individual" responsible for developing, overseeing, monitoring, and enforcing an information security program.
- The designated "Qualified Individual" needs to report in writing, at least annually, to the company's board of directors or owner.
- Periodic risk assessments need to be used to guide continued updating and enforcement of your information security program.
- Implement customer information safeguards to control the risks identified in the risk assessments.
- Implement policies and procedures to ensure employees correctly carry out the information security program.
- Ensure that service providers or third parties that have access to their customer information maintain safeguards commensurate with your business's information security program.
- Have a written incident response and mitigation plan to lay out the process for responding to any breach of your information systems or exposure that compromises customer information that is maintained.
- Notifications of regulatory government agencies of cybersecurity incident at state and federal levels.
- Notification of cybersecurity incident that complies with laws of the states the customers live in

The LibertyID Solution

- Information Security and Response Planning (WISP)
- Regulatory Response and Client Notification
- Customer Identity Fraud Restoration Services
- Web Domain Monitoring
- Risk Assessments
- Policies and Procedures
- Vendor Assessments
- Employee Training and Testing
- Employee and Family Identity Fraud Restoration Concierge Services
- Business Fraud Restoration
- Customer Identity Fraud Restoration Concierge Services

CYBERFIN