FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches

Agency updates Safeguards Rule to better protect the American public from breaches and cyberattacks that lead to identity theft and other financial losses

Compliance deadline extended to June 2023

FTC Definition: "Financial institution means **any institution the business of which is engaging in an activity that is financial in nature** or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C § 1843(k). An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution."

In addition to banks, brokerage firms and insurers, the Gramm-Leach-Bliley Act (GLBA) applies to companies that process loans or otherwise assume credit risk. Any organization that falls within the scope of GLBA must comply with its provisions, although individual states have the power to enact more stringent privacy regulations, as is the case in California and Virginia.

Professions and businesses subject to GLBA's provisions include, but may not be limited to:

- Accountants
- ATM operators
- Car Rental Companies
- Courier Services
- Credit Unions
- CPA Firms
- Payday Lenders
- Property Appraisers
- Real Estate Firms
- Retailers
- Stockbrokers
- Tax Preparers
- Universities
- Debt Collectors
- Financial Advisors
- Credit Reporting Companies
- Non-bank Mortgage Lenders
- Hedge Funds

Review the official PDF from the Federal Trade Commission:
https://www.irs.gov/pub/irs-pdf/p4557.pdf
Protecting Personal Information: A Guide for Business
https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business
"The FTC can and does take law enforcement actions..."
https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement
Fines of $11,000 per day per Occurrence of Breach

6 Quick Questions:

- Have you conducted regular **risk assessments** or "penetration testing" by a qualified third party?
- Are your staff properly **trained on security** and participating in ongoing simulated phishing attacks?
- Are your computer drives and **files encrypted** and are you sending sensitive files using **encrypted email**?
- Can you log in to your business email or network without being prompted for a **verification code or multi-factor authentication on your phone**? (hint: you shouldn't)
- Do you have the **skills**, **experience** and **time** to conduct the work properly in accordance with FTC guidelines?
- **Have you viewed any of the above links??**
  No? "Procrastination of the Thief of Time!"