ATTACHMENT A

institutions[7] to make disclosures about their information sharing practices and to implement a comprehensive information security program to protect consumer information.[8] Similarly, the Fair and Accurate Credit Transactions Act ("FACTA"), enacted in 2003, supplements longstanding U.S. credit laws to establish requirements for the masking, sharing, and disposal of certain sensitive financial data. The FTC promulgated a number of rules under FACTA regarding, among other things, consumers' right to a free annual credit report; secure disposal requirements for consumer report information; consumers' right to opt out of receiving certain offers of credit and insurance; consumers' right to opt out of the use of information provided by an affiliated company to market its products and services; and requirements for financial institutions and creditors to implement identity theft detection and prevention programs.[9] In addition, rules promulgated under the Health Insurance Portability and Accountability Act were revised in 2013, adding additional safeguards to protect the privacy and security of personal health information.[10] Rules protecting consumers from unwanted telemarketing calls, robocalls, and spam have also gone into effect. Congress has also enacted laws requiring certain companies that collect health information to provide consumers with notification in the event of a breach.[11]

States have also been very active in passing laws related to privacy and security. Since 2000, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted laws requiring businesses to notify individuals of security breaches of personal information.[12] At least thirty-two states and Puerto Rico have data disposal laws, establishing requirements for the destruction or disposal of personal information.[13] A number of states also have enacted general data security laws. In addition, California has enacted various privacy laws, including a law requiring companies to have privacy policies and disclose their Do Not

---

[7] Financial institutions are defined very broadly under the Gramm-Leach-Bliley Act to include all businesses that are "significantly engaged" in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and professional tax preparers.

[8] Under the Consumer Financial Protection Act of 2010 ("CFPA"), Title X of Pub. L. 111-203, 124 Stat. 1955 (July 21, 2010) (also known as the "Dodd-Frank Wall Street Reform and Consumer Protection Act"), most of the FTC's Gramm-Leach-Bliley Act rulemaking authority was transferred to the Consumer Financial Protection Bureau ("CFPB"). The FTC retains enforcement authority under the Gramm-Leach-Bliley Act as well as rulemaking authority for the Safeguards Rule and limited rulemaking authority under the Privacy Rule with respect to auto dealers.

[9] Under the CFPA, the Commission shares its FCRA enforcement role with the CFPB, but rulemaking authority transferred in large part to the CFPB (with the exception of the Red Flags and Disposal Rules).

[10] *See* 45 C.F.R. pts. 160, 162, 164.

[11] *See, e.g.*, American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) and relevant regulations, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. pt. 318.

[12] *See, e.g.*, National Conference of State Legislatures ("NCSL"), *State Security Breach Notification Laws* (Jan. 4, 2016), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx .

[13] NCSL, *Data Disposal Laws* (Jan. 12, 2016), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

Track practices,[14] a "Shine the Light" law requiring greater transparency for data brokers,[15] and a law that mandates an "eraser button" allowing minors to request the deletion of certain social media information.[16] Using these laws and other authorities, federal and state governments have levied significant fines against companies that have failed to protect the privacy and security of consumers' personal information.[17]

Private lawsuits have also led to successful judgments and settlements that provide additional privacy and data security protection for consumers. For example, in 2015, Target agreed to pay $10 million as part of a settlement with customers who claimed their personal financial information was compromised by a widespread data breach. In 2013, AOL agreed to pay a $5 million settlement to resolve a class action involving alleged inadequate de-identification related to the release of search queries of hundreds of thousands of AOL members. Additionally, a federal court approved a $9 million payment by Netflix for allegedly keeping rental history records in violation of the Video Privacy Protection Act of 1988. Federal courts in