Data Breach Prevention and Compensation Act

In 2017, Equifax announced that hackers had stolen sensitive personal information—including Social Security numbers, birth dates, credit card numbers, and driver's license numbers—from over 145 million Americans. The attack highlighted that credit reporting companies (CRCs) hold vast amounts of data on millions of Americans and lack adequate safeguards against hackers. Press reports and cybersecurity experts identified a number of security lapses at Equifax—including in the days following the company's disclosure of the breach—which potentially indicate a pattern of security failings. Consumers are still inadequately protected, in 2024, seven years after that massive data breach.

The Data Breach Prevention and Compensation Act addresses this problem by giving the Federal Trade Commission more direct supervisory authority over data security at CRCs and imposing a strict liability penalty regime that will incentivize the largest agencies to adequately protect consumer data and automatically compensate consumers for stolen data. Specifically, the bill:

- Imposes strict liability penalties for breaches involving consumer data at credit reporting agencies. CRCs—including Equifax—currently face no mandated penalty for allowing consumer data to get stolen after they have collected it without consent. This bill imposes mandatory, strict liability penalties for breaches of consumer data at CRCs, beginning with a base penalty of $100 for each consumer who had one piece of personal identifying information (PII) compromised, with an additional $50 for each additional piece of PII compromised per consumer. The bill caps the penalty at a maximum of 50% of the CRC's gross revenue from the prior year.

- Ensures robust recovery for affected consumers. Under current law, it is difficult for consumers to get compensation when their personal data is stolen. Typical awards range from $1 to $2 per consumer. This bill requires the FTC to use 50% of its penalty to compensate consumers.

- Establishes an Office of Cybersecurity at the FTC that is tasked with annual inspections and supervision of cybersecurity at CRCs. The FTC currently does not have adequate authority or resources to monitor data security practices at CRCs. This bill establishes a Director and Office of Cybersecurity to conduct cybersecurity inspections at CRCs and authorize the FTC to promulgate new regulations outlining effective data security standards for CRCs. It also orders the FTC to report to Congress on areas where it needs to enhance the agency's authorities to fully address cyber-theft.

- Increases penalties for cases of woefully inadequate cybersecurity or failure to notify. The bill doubles the automatic per-consumer penalties and increase the maximum penalty to 75% of the CRC's gross revenue in cases where the offending CRC fails to comply with the FTC's data security standards or fails to timely notify the agency of a breach.