LEADERSHIP CENTER FOR ATTORNEY GENERAL STUDIES

DATA BREACHES ISSUE BRIEF

Background

A data breach occurs when there is the unlawful and unauthorized acquisition of personal information from a computer or other filing system. These breaches threaten the security, confidentiality, and integrity of personal information. Often such breaches put consumers and constituents at risk for identity theft.

Data breaches that involve personal information are most concerning. Personal information is often defined as someone's name plus one of the following: social security number, driver's license number, credit card number, financial account number, biometric information (defined as information about a person's unique physical characteristics), email address and password, tax identification numbers, health information, or log in credentials.

Role of State Attorneys General

State Attorneys General are on the front lines when consumers' data is breached. Attorneys General are often asked by their constituents what they can do. Attorneys General have two important enforcement powers: (1) state data breach statutes; and (2) the authority to enforce state consumer protection statutes that prohibit unfair trade practices.

State Data Breach Statutes

All 50 states, DC, Guam, Puerto Rico, and the U.S. Virgin Islands have data breach notice laws. Generally, these statutes require companies that suffer a data breach to provide timely notice to the state attorney general and impacted consumers. This timely notice provides attorneys general and impacted consumers the ability to prevent further harm caused by breach, such as identity theft. For consumers, this notice allows consumers to monitor their credit and other financial accounts for suspicious activity. Attorneys General that receive notice can conduct investigations and enforcement actions to deter further unlawful activity caused by the breach. There are variations amongst state data breach laws, including whether notification of a breach depends upon a risk assessment of potential harm and whether the underlying data was encrypted. Generally, remedies available to attorneys general under these statutes, which often incorporate remedies from their states' respective consumer protection laws, include injunctions requiring companies to take steps to protect consumer data, update systems, and improve corporate governance. In addition, attorneys general can seek consumer restitution including free credit monitoring, civil penalties, attorneys fees and costs.

State Consumer Protection Statutes

The second source of authority for attorneys general to protect consumers from data breaches are consumer protection acts that prohibit unfair and deceptive practices. Generally, an unfair trade practice occurs when a practice offends public policy, is oppressive or unscrupulous, or causes substantial injury to consumers. Failing to adequately protect data security is an unfair trade practice because it could substantially injure consumers if their personal information is compromised as a result of a breach. When companies experience a data breach because of a failure to employ adequate security protocols, including failure to utilize complex passwords, failure to implement timely patches of

IT system vulnerabilities, and otherwise fail to maintain a comprehensive security system to keep customers' information safe, they will be subject to investigations and enforcement action by Attorneys General. The courts and regulators have determined that the failure to adequately protect consumers' personal information amounts to an unfair trade practice. For instance in 2011, a U.S. District Court recognized that "a court could find that the company's lack of security measures constitutes an unfair practice because such conduct is systematically reckless, 'aggravated by [a] failure to give prompt notice when lapses were discovered internally, and causing very widespread and serious harm to other companies and to innumerable consumers.'" This is the same position also taken by attorneys general with several recently entering into two settlements after incidents of data breaches where it was alleged that the failure to maintain adequate data protection amounted to an unfair trade practice.

Recent Examples of State Attorney General Actions:

Several examples of settlements reached by Attorneys General in multi-state investigations involving data breaches include:

- A $16 million settlement announced in November, 2022, resolving a multi-state investigation into Experian and T-Mobile's failure to protect consumer data. The underlying data breach involved an unauthorized actor gaining access to Experian's network that stored personal information on behalf of its client, T-Mobile. The breach involved consumers' names, addresses, dates of birth, social security numbers, and other identification numbers. As part of the settlement, Experian also agreed to provide five years of free credit reporting services to affected consumers.

- In June 2022, attorneys general from 46 states announced a $1.25 million settlement with Carnival Cruise Line (Carnival) to resolve a multi-state data breach investigation. The investigation involved allegations that an unauthorized user accessed Carnival employees' email accounts and obtained customer names, addresses, passport numbers, driver's license numbers, payment card information, health information, and social security numbers. Carnival became aware of the breach in May 2019, but did not report it for approximately 10 months. Carnival also agreed to maintain a comprehensive data security program, implement data retention policies, adopt multi-factor authentication policies, employ encryption, implement employee training, and undergo an independent security assessment.

- 50 attorneys general secured a $600 million settlement with Equifax in 2019 after it suffered a massive data breach affecting 150 million consumers. The multi-state investigation found that Equifax failed to institute adequate security measures. It knew about, but failed to correct critical vulnerabilities in its software. As a result, there was a significant release of consumer personal information including social security numbers, dates of birth, addresses, driver's license numbers, and credit card numbers. Equifax agreed in the settlement to minimize collection of sensitive consumer data, perform regular security monitoring, and enhance its security patch management. Equifax also agreed to provide credit monitoring, adopt policies to make it easier for consumers to freeze and thaw their credit, dispute inaccurate credit information, and maintain dedicated staff to assist consumers who may be victims of identity theft.

LEADERSHIP CENTER FOR ATTORNEY GENERAL STUDIES

The Leadership Center for Attorney General Studies is a non-partisan organization dedicated to educating the public about the important role state attorneys general play in addressing pressing issues, enforcing laws, and bringing about change.