Retailers' Position on Data Breach Legislation

ISSUE

Congress is considering legislation that would govern how businesses protect sensitive consumer data such as Social Security, driver's license, bank account and credit card numbers, and how consumers are notified if that data is breached. NRF strongly supports creation of a uniform national data breach notification law that would replace a patchwork of 50 conflicting state laws.

Consumers would be best helped by a data breach law which ensures they are notified no matter where a data breach might occur, whether it's at a retailer, bank, credit card company, data service provider or elsewhere. NRF believes the new law should cover all entities that handle sensitive consumer data and should not provide an exemption from breach notification rules for any business.

IMPACT ON RETAILERS

Breaches affect every industry and well-respected breach investigation reports have shown for the past several years that retailers suffer just five percent of all breaches that have data loss. But data thefts committed against retailers receive the most attention because retail stores are household names consumers recognize and shop at every day. Additionally, many state data breach laws require only consumer-facing companies, like retailers, to notify the public of breaches without requiring banks or service providers in the telecom or technology sectors to do the same. This leads to the incorrect assumption that retailers are responsible for most breaches, leaving consumers unaware of thousands of non-retail breaches every year that put them at risk of identity theft or financial harm.

In fact, protecting customer data is one of retailers' top priorities. Retailers spend millions of dollars a year on data security, establishing extensive firewalls, hiring world-class cybersecurity experts and encrypting their card payment data. For example, an NRF survey found that by the end of last year, 93 percent of retailers were expected to adopt point-to-point encryption, which protects card data while it is being transmitted.

HOW CONGRESS CAN HELP

Since 2005, NRF has worked with members of the Energy and Commerce Committee to craft federal legislation that would create a uniform, national requirement for all breached businesses to provide notice of their breaches to affected individuals. We believe that preemptive federal data breach legislation is not only necessary but also politically achievable provided that it adopts three essential principles that NRF strongly supports:

1. **Federal Legislation Must Cover ALL Entities Handling Sensitive Personal Information:**
   All entities – from well-recognized consumer brands to "behind-the-scenes" third-party service providers and data brokers – handling sensitive personal information should have the same obligations to protect that data and notify affected individuals when suffering a breach of security.

2. **Federal Legislation Should Create a Uniform, Nationwide Data Breach Disclosure Standard:**
   All 50 states and four federal territories already have breach notification laws. It is time for Congress to create a sensible, uniform breach notification regime that benefits consumers and businesses by ensuring that all affected individuals are notified in a consistent and timely manner no matter when or where a breach of security occurs. Without effective preemption, Congress would simply add a 55th set of requirements to what is already an unworkable framework for interstate commerce.

3. **Data Security Standards Should be Reasonable and Based on the Use and Sensitivity of Data:**
   Businesses subject to FTC jurisdiction are remarkably diverse in their size and scope of operations, and they differ greatly with respect to their use of customer information and the sensitivity of the data they process. For these reasons, one-size-fits-all data security standards are unworkable. Legislation should authorize the FTC to enforce reasonable data security standards, which would provide necessary flexibility in its application to the diverse set of businesses to which these standards would apply.