February 8, 2018

The Honorable Floyd Prozanski
Chairman, Senate Committee on Judiciary
Oregon State Legislature
900 Court Street, NE
Salem, OR 97301

Dear Chairman Prozanski and Members of the Committee:

The National Retail Federation (NRF) appreciates the opportunity to provide its views to the Committee on SB 1551. This legislation is intended to protect consumer data in light of data security breaches that have occurred, including most recently at Equifax. NRF supports public policy that requires *all* businesses to provide notice of their data breaches to affected individuals. However, SB 1551 in its current form would exempt entities which handle the most sensitive information from providing breach notice to affected Oregonians in most instances. In addition, the bill would impose data security standards designed to protect the most sensitive financial information on businesses handling less sensitive data, which poses less risk to consumers. For these reasons, as discussed further below, we oppose the legislation in its current form.

NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing $2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy. In the state of Oregon, there are over 48,000 retail establishments supporting approximately 537,850 jobs.

According to the 2017 Verizon Data Breach Investigations Report, all sectors of U.S. industry are affected by security breaches, but one in particular accounts for nearly a quarter of all breaches, defined as security incidents with confirmed data loss. Verizon reported that the financial services sector had 24.3% of all breaches during the previous year, which is not surprising since banks and credit unions also handle American's most sensitive personal information, and the hackers know this. By contrast, businesses with less sensitive data generally account for fewer breaches, and Verizon reported, for instance, that the retail industry suffered just 4.8% of all breaches. (Please see the attached graph that depicts where breaches happen based on the data in Verizon's report.)

We believe that legislation requiring notice for breaches of consumer data should cover all entities handling sensitive personal information. Whether they handle consumer data through direct contact with customers or as third-party service providers, all entities should have obligations to protect that data and notify affected consumers when they suffer a breach of security. Security breaches affect all industry sectors and we support the principle that the entity that suffers a breach should be the one that bears responsibility for notifying affected consumers of that breach. However, SB 1551 would

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com

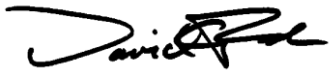
be unique among 48 existing state laws by putting all of the breach notification obligations onto just those businesses accepting payment cards, even if a breach occurs elsewhere in the payment system. To protect consumers comprehensively, any data breach law must apply to all industry sectors and place public disclosure responsibility where it belongs – on the entity that suffered the breach of security affecting individuals' sensitive personal information.

Furthermore, data security standards must be appropriately tailored to a business's size and scope of operations, and the sensitivity of the consumer data it handles. Given the breadth and diversity of consumer-facing businesses, the most appropriate data security standard for non-financial institutions, like merchants and restaurants, is one based on reasonableness. The Federal Trade Commission (FTC), for example, has long held that "reasonable data security" is most appropriate for businesses that are not engaged in financial activities and it has held that mere acceptance of card payments does not constitute financial activity. SB 1551, however, proposes to place standards designed for banks with assets exceeding $10 billion and for credit bureaus, like Equifax, onto companies holding much less sensitive information than those in the financial services industry.

We respectfully urge this Committee to reject SB 1551 and work to craft comprehensive legislation that requires all entities suffering a security breach to provide notice to affected individuals and to implement reasonable data security standards appropriate for the type and sensitivity of data they handle. The legislation, as currently drafted, instead creates "notice holes" (or exemptions) for certain favored industries and would establish an unworkable "one-size-fits-all" data security requirement for a wide range of Main Street businesses based on federal banking standards appropriate only for large financial entities handling consumers' most sensitive financial information.

Thank you for the opportunity to provide you with our views on the proposed legislation and we look forward to working with this Committee and the Oregon legislature on this issue in the future.

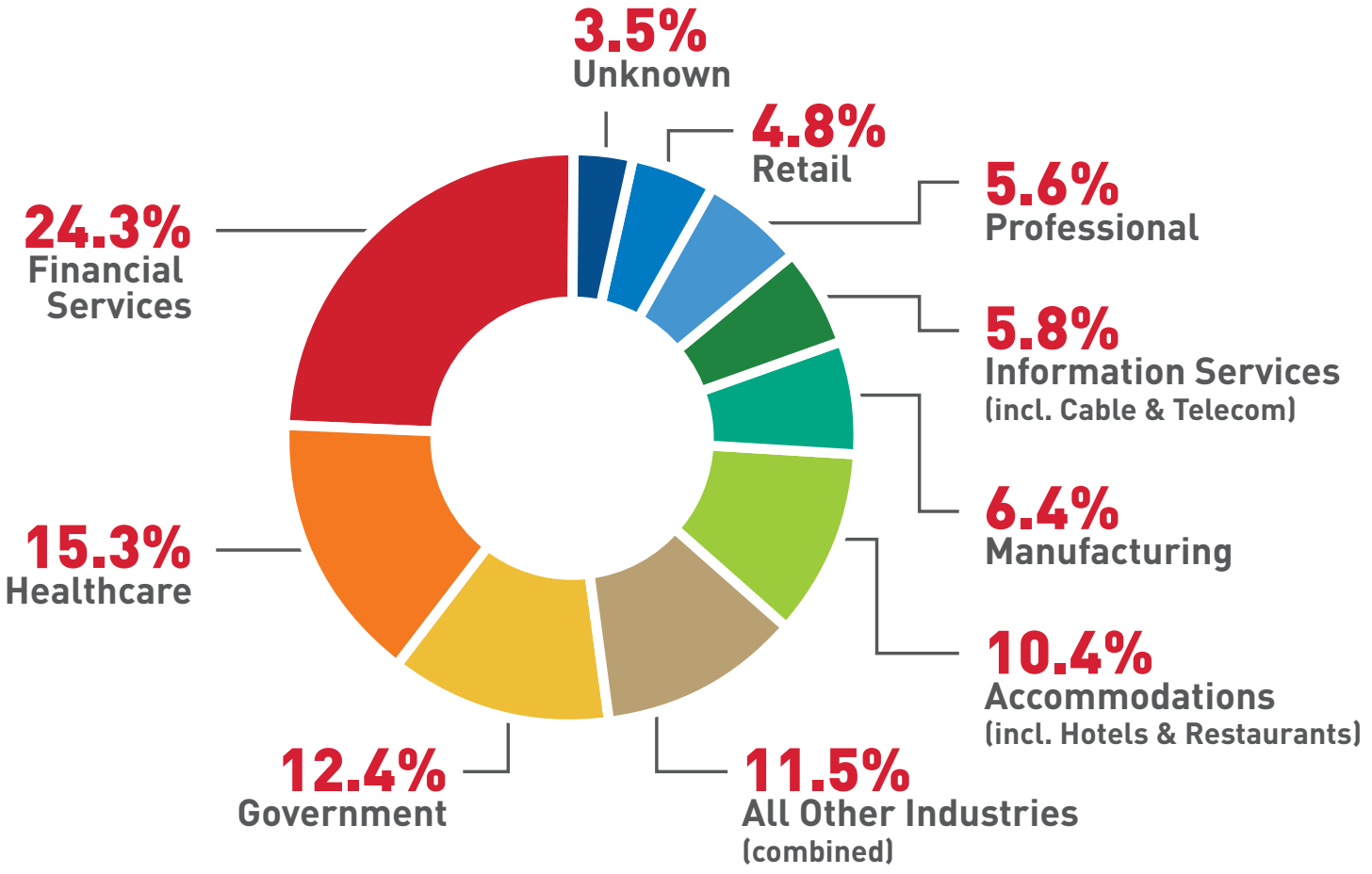
Sincerely,



David French
Senior Vice President
Government Relations

attachment

Where Breaches Happen



Source: Verizon 2017 Data Breach Investigations Report

NRF® NATIONAL RETAIL FEDERATION®

COM-014

nrf.com/datasecurity