

Harold B. Scoggins, III
Attorney
Admitted in Oregon and Washington

hscoggins@fwwlaw.com

121 SW Morrison Street, Suite 600
Portland, Oregon 97204

tel 503.228.6044
fax 503.228.1741

www.fwwlaw.com

March 27, 2017

**TESTIMONY
IN SUPPORT OF HB 2581
PRESENTED BY HAROLD B. SCOGGINS, III
FARLEIGH WADA WITT
Counsel for the Northwest Credit Union Association
Before the House Committee
On Business and Labor**

Good afternoon Chair Holvey and members of the committee, my name is Harold Scoggins. I am an attorney with Farleigh Wada Witt, outside counsel for the Northwest Credit Union Association. Our firm also represents many individual credit unions throughout Oregon and Washington and the Western U.S. I appreciate the opportunity to talk with you today about HB 2581. I will provide some background information related to the bill and will be happy to answer questions.

Current Oregon Law

Currently Oregon law, specifically ORS 646A.600-628, addresses data security in three ways:

(i) It imposes information security requirements on organizations holding sensitive personal information (organizations like credit unions and banks that are subject to federal regulations under the Gramm Leach Bliley Act are deemed to comply with Oregon law if they comply with applicable federal requirements);

(ii) It requires organizations to notify consumers (and in some cases the Oregon Attorney General) affected by a data breach; and

(iii) It allows consumers to place a security freeze on their credit reports.

Proposals from Around the Country

Financial institutions, consumers, merchants, and legislatures around the country have taken a number of different approaches to address the growing problem of card data breaches at retailers. Some proposals require an organization that fails to adhere to security standards and has a breach to offer free credit monitoring for affected consumers for a period of time. Others impose make organizations that fail to adhere to security standards and have a breach liable to affected consumers or financial institutions. Some provide state authorities with

the power to impose civil penalties on organizations that do not comply with information security requirements. And some impose additional notice requirements for organizations that suffer a breach, requiring notice to consumers, authorities, or affected financial institutions.

Protections in this Bill

As originally introduced, this bill did three things: a) it required organizations suffering a breach involving card data to notify their transaction processor and affected financial institutions; b) if an organization did not adhere to appropriate data security standards, it made the organization liable to affected financial institutions for costs associated with the breach (including for example, costs of providing notice to affected cardholders, costs to reissue cards, etc.); and c) it authorized the Department of Consumer and Business Services to prescribe data security standards that organizations must meet in order to avoid liability.

The -1 amendments will delete the liability provision and the related DCBS authority to prescribe data security standards. Thus, if the -1 amendments are adopted, the bill will have a single operative purpose: requiring merchants that suffer a breach of card data to provide notice to affected financial institutions. Once a merchant discovers that there has been a breach, the merchant will review its records and conduct an investigation to determine what records were subject to the breach. Working with its card transaction processor, the merchant will determine which financial institutions held the cards subject to the breach. Contact information for financial institutions is readily available from federal regulatory websites. The merchant can then provide notice to the affected institutions using a method that is most convenient to the merchant. The notice could be provided on paper using redacted information, or via encrypted media, or the merchant could notify the institution to contact the merchant to arrange for secure email transfer.

The bill (as amended) will not alleviate the substantial losses that a credit union suffers when its cardholders are subject to merchant data breaches. However, it will perhaps make merchants more aware of the cost and inconvenience of such breaches and may in turn create an impetus for improved security measures. It will also provide financial institutions with better notice of breaches – avoiding the delay and sometimes complete omission of notice provided through the card networks. This may permit institutions to act more quickly to prevent fraud losses from occurring.

P:\DOCS\NWCUA\01199\DOC\3PX9427.DOC