Northwest Credit Union Association
Idaho • Oregon • Washington

www.nwcua.org

Comments on HB4147 – House Business and Labor Committee
February 7, 2018

The Northwest Credit Union Association represents the 59 state and federally-chartered credit unions in Oregon, with 2 million Oregonians as members. Credit unions are not-for-profit financial cooperatives, organized to meet the financial needs of their members. As member-owned cooperatives, Oregon credit union's take their responsibility to protect member information extremely seriously, and diligently work to comply with state and federal regulations.

Although most consumers have probably only heard about a few breaches, hundreds of retail security breaches occur each day, exposing millions of data records. Consumers will be protected from fraudulent charges on their cards due to a breach, and the cost is generally picked up by the financial institution. Financial institutions are limited by law in disclosing many of the circumstances of a data breach. In addition, financial institutions protect consumers when a merchant data breach occurs by informing members and customers and reissuing new credit and debit cards believed to have been compromised.

The Northwest Credit Union Association supports state and federal legislation to address the significant and growing problems associated with data security breaches that compromise the confidentially of financial and personal information of credit unions and their members. Here are just a couple examples of costs to Oregon credit unions:

**Oregon State Credit Union Background**

In 2016, Visa notified the credit union of more than 300 distinct breach alerts at businesses of all sizes and types. Those often don't include the small local breaches. One such very small local retail business was naively compromised through their use of an unsecure Wi-Fi used at their transaction point. **Overall in 2016, approximately 4,200 cards were reissued and incurred hard costs of approximately 563,000.** That does not include staff time and the pursuit of criminals through available legal channels saving the member time and expenses.

**OnPoint Community Credit Union Background**

During 2016, OnPoint identified 301 card compromises that impacted 58 thousand cards/members. Over 32 thousand cards were affected in a single data breach that occurred at a national chain. Each time an identifiable card beach occurs, OnPoint cancels and reissues thousands of plastic cards to our members. In 2016, this totaled $535,000 for the credit union.

**Equifax**

Equifax, one of the big three U.S. credit bureaus announced on Thursday, Sept. 7, 2017, that a data breach at

the company may have exposed 143 million American consumers' sensitive personal information. Although Equifax states they found no evidence of unauthorized activity on its core consumer credit reporting database, other information was lost. According to Equifax, the breach lasted from mid-May through July. The hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. This is the sensitive information fraudsters need to commit identity theft.

**HB4147**

We appreciate Chair Holvey's work on this issue and bringing to light the many issues associated with data breach. We support efforts that will help financial institutions receive notice of a breach as soon as possible, however we oppose Section 2 (2)(b) that adds new language for a financial institution to report a possible breach. Here are our arguments against Section 2 (2)(b):

In short, this language imposes UTPA liability on a financial institution for failing to report a breach that it likely cannot discover, to a party that it cannot identify. There are several specific problems:

First, it is unclear when a financial institution would be deemed to "discover" or "receive notice" of a breach that triggers this notification requirement. For example, if credit union member makes a deposit to their account and says to the drive-in teller "I heard that the hardware store had a data breach," does that trigger a reporting requirement? Financial institutions do not have access to a merchant's data systems, processes, or transaction information. The only way a financial institution could independently discover a breach is through detective work that is ordinarily performed by other parties. The most information a credit union would have is some possible knowledge that high levels of card fraud have occurred among cardholders who went to a specific merchant. But even then, there are usually multiple common merchants among cardholders who have experienced fraud.

Also, the new language requires reporting to the merchant services provider that processed a transaction involving the information subject to the breach. While the credit union can identify the merchant that received the funds, it has no means to identify the processor that performed services for the merchant. The merchant services provider is contracted for by the merchant, not the financial institution. The transaction is processed through the payment card network (i.e. Visa or Mastercard). Also, a credit union may learn (through law enforcement or through the payment network) that a merchant suffered a breach, but it has no information about which cards were involved in the breach. The only way the credit union gets that information now is when the payment network makes a report indicating that specific cards have been compromised.

The bill imposes UTPA liability for failing to adhere to the notice provisions, including this specific notice requirement. It is patently unfair and inappropriate to subject a credit union (which had nothing to do with the breach and which will likely not be aware of the breach until long after the merchant is) to UTPA liability for failing to comply with this notice requirement. A merchant that has suffered a breach will be aware of that breach long before any financial institution. Our request had been to adopt provisions that will more quickly get information about a breach into the hands of the party best equipped to prevent fraudulent card transactions (the issuing financial institution, which bears the brunt of the losses). The above language does nothing to address that issue.

*Contact: Pam Leavitt, Leavitt.nwadvocacy@gmail.com, 503-887-2336*