

HOUSE BILL REPORT

HB 1888

As Reported by House Committee On:
Technology, Energy & Communications

Title: An act relating to electronic mail fraud.

Brief Description: Regulating electronic mail fraud.

Sponsors: Representatives Nixon, Morris, Hunter, B. Sullivan, Simpson, Ormsby, Morrell, Haler, Clibborn, Ericks, Williams, Darneille, Dunn, Dickerson, P. Sullivan, Green and Hudgins.

Brief History:

Committee Activity:

Technology, Energy & Communications: 2/15/05, 2/17/05 [DPS].

Brief Summary of Substitute Bill

- Prohibits a person from misrepresenting his or her identity in order to solicit another person to provide personally identifying information by means of a web page, electronic mail, or the internet.

HOUSE COMMITTEE ON TECHNOLOGY, ENERGY & COMMUNICATIONS

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 11 members: Representatives Morris, Chair; Kilmer, Vice Chair; Crouse, Ranking Minority Member; Haler, Assistant Ranking Minority Member; Ericks, Hudgins, Nixon, P. Sullivan, Sump, Takko and Wallace.

Staff: Kara Durbin (786-7133).

Background:

Unsolicited E-mail:

In 1998, legislation was enacted regulating commercial electronic mail (e-mail) messages, collectively referred to as "spam." A commercial electronic mail message is an e-mail message sent for the purpose of promoting real property, goods, or services for sale or lease. In particular, the laws prohibit the sending of commercial e-mail from a computer located in Washington to an e-mail address of a Washington resident if the commercial e-mail uses:

- a false or misleading return address;
- a false or misleading subject line; or

- a third party's e-mail address (domain name) without permission.

The law not only prohibits the sender from sending a false or misleading commercial e-mail message, but also prohibits anyone who conspires with the sender or who assists in the transmission of the commercial e-mail message. A sender is responsible for knowing that a recipient is a Washington resident, if that information is available, upon request, from the registrant of the internet domain name contained in the recipient's electronic mail address, typically the internet service provider. The Attorney General and the Washington Association of Internet Service Providers have established a voluntary on-line registry where a Washington resident can register their e-mail address.

An interactive computer service (which includes internet service providers) may block the transmission of commercial e-mail that it reasonably believes is being sent in violation of the law and may not be held liable for this voluntary action taken in good faith.

A recipient or an internet service provider may bring a civil action against a sender who violates the laws relating to commercial electronic mail messages. In the case of a suit brought by a recipient, the penalty is the greater of \$500 or actual damages incurred. In the case of a lawsuit brought by an internet service provider, the penalty is the greater of \$1,000 or actual damages. A violation of laws relating to commercial electronic mail messages is also a violation of the Consumer Protection Act and may be enforced by the Attorney General. A violation of the Consumer Protection Act may result in a civil fine, treble damages, court costs, and attorneys' fees.

Phishing:

The term "phishing" generally refers to a type of internet activity that uses fraudulent e-mails and websites to solicit personal financial information from an e-mail recipient. Typically, a user receives an e-mail that appears to be from a familiar business or organization, such as an internet service provider, bank, or online retailer. The message usually requests that the recipient update or validate his or her account information by clicking on a link embedded in the e-mail. Once the recipient clicks on the link, the user is taken to a fraudulent website where the user is asked to input personal and confidential information.

Summary of Substitute Bill:

This law prohibits a person from soliciting, requesting, or taking any action to induce another person to provide personally identifying information by means of a web page, electronic mail message, or otherwise using the internet by representing oneself, either directly or by implication, to be a business or individual without the authority or approval of such business or individual.

"Personally identifiable information" is defined as any of the following types of information:

- Social Security Number;
- driver's license number;

- bank account number;
- credit or debit card number;
- Personal Identification Number;
- automated or electronic signature;
- unique biometric data;
- account passwords; or
- any other piece of information that can be used to access an individual's financial accounts or to obtain goods or services.

A consumer can seek damages of up to \$500 per violation, or actual damages, whichever is greater.

An internet service provider, an owner of a web page, or a trademark owner can seek to enjoin further violations, and may recover \$5,000 per violation, or actual damages, whichever is greater. In addition, the court may increase the damage award up to three times (up to \$15,000) if the defendant has engaged in a pattern and practice of engaging in the prohibited activities. The court may also award costs and reasonable attorneys' fees to the prevailing party.

A violation of these provisions is defined as an unfair or deceptive act for purposes of applying the Consumer Protection Act.

There is a severability clause.

Substitute Bill Compared to Original Bill:

Makes a technical change to the bill, to clarify that this section prohibits a person from representing themselves to be a business or individual when that person does not have the authority or approval of such business to do so.

Appropriation: None.

Fiscal Note: Not requested.

Effective Date of Substitute Bill: The bill takes effect 90 days after adjournment of session in which bill is passed.

Testimony For: This is a widespread problem. Many computer users receive multiple fraudulent e-mails per day. These phishing e-mails create a sense of urgency and look very real. It is very easy for phishers to forge e-mail addresses. Often, the link the computer user sees on his or her screen is not where the link actually goes to. The fake site looks almost identical to the real site. Financial institutions support this bill because ultimately it is their customers that are the bait. The banks often have to bear some of the costs. This bill is needed because it is estimated that phishing-related losses will exceed \$150 million in Washington this year.

Testimony Against: None.

Persons Testifying: Representative Nixon, prime sponsor; Gary Gardner, Boeing Employees Credit Union and Washington Association of Internet Service Providers; Denny Eliason, Washington Bankers Association; and Steve Larsen, Office of the Attorney General, High-Tech Section.

Persons Signed In To Testify But Not Testifying: None.