SUBJECT: Prohibiting Internet "phishing" fraud

COMMITTEE: Regulated Industries — favorable, as amended

VOTE: 6 ayes — P. King, Hunter, Turner, R. Cook, Crabb, Hartnett

0 nays

1 absent — Baxter

WITNESSES: For — James Hines, MCI; Luke Metzger, Texas Public Interest Research Group; Andrew Wise, Microsoft Corp., (*Registered but did not testify*: Grisalda Camacho, American Electronics Association; John Fainter, Association of Electric Companies of Texas, Inc.; Neal Jones, Microsoft; Jennifer Shelley Rodriguez, Apple Computer; Melodie Stegall, Credit Union Legislative Council; Ray Sullivan, eBay, Inc.)

Against — None

DIGEST: HB 1098, as amended, would prohibit obtaining personal identifying information of other individuals through certain means via the Internet with the intent to possess or use such information fraudulently. The bill would prohibit:

- creating a Web page or Internet domain name representing a legitimate online business without the business owner's authority; and
- using that Web page or domain name to solicit from another person identifying information.

The bill also would prohibit ending an e-mail that:

- falsely represented itself as being sent from a legitimate business;
- referred the recipient to a falsely represented Web site; and
- solicited from the recipient identifying information for a purpose that the recipient believe d to be legitimate.

Identifying information would be defined as any information that identified an individual, such as a name, social security number, date of

birth, address, driver's license number, bank account number, check routing number, personal electronic identification number (PIN), credit card number, or phone number.

A person committing such an offense would be committing a state jail felony (180 days to two years in a state jail and an optional fine of up to $10,000). A repeat offense would be a third-degree felony (two to 10 years in prison and an optional fine of up to $10,000).

In addition, certain parties could bring civil action under this bill. Those parties would include:

- an Internet access provider who was harmed by a violation under this bill;
- an owner of a Web page or trademark who was harmed by a violation under this bill; or
- the attorney general of Texas.

A person bringing action could seek injunctive relief to halt a violation under this bill, recover damages in the greater amount of the actual damages arising from the violation or $100,000 for each violation of the same nature, or seek both injunctive relief and recover damages. Violations would be of the same nature if they consisted of the same action or course of conduct, regardless of how many times the act occurred. A court could increase damages to three times the actual damages sustained if violations constituted a pattern. A prevailing plaintiff could collect attorney's fees and court costs.

The bill would take effect September 1, 2005.

SUPPORTERS SAY:

HB 1098 would expressly prohibit the practice of "phishing," a widespread form of identify theft that uses fraudulent email messages and Web sites to trick citizens into forfeiting sensitive personal information.

Currently an e-mail user can receive a message from a sender purporting to represent the user's bank, credit card company, or other business directing the recipient to visit a Web site. Once the recipient visits that site, the user is requested to enter his or her social security number, bank account number, or other information, believing that this data will be used for legitimate business purposes. However, the operator of this Web site could be an impersonator, collecting this identifying and financial data for

fraudulent purposes. Unsuspecting, innocent individuals unknowingly are providing criminals with access to sensitive personal data, and they need the protection provided that HB 1098 would provide.

Identity theft is a substantial problem in the United States, and phishing represents the cutting edge of this devious practice. The Federal Trade Commission reports that in 2003 almost 10 million Americans were victims of identity theft. According to the Anti-Phishing Working Group, the volume of fraudulent, phishing e-mail is growing at a rate in excess of 30 percent each month. While Internet-based communications have improved business efficiency and the capability for social interaction, the proliferation of e-mail also has enabled innovations in criminal fraud. Specific legislation is necessary to stem the tide of these abusive practices.

Phishing harms both individuals who lose confidential data and companies whose legitimate identities are compromised, and HB 1098 would provide protection for both sets of victims. The list of companies whose identities have been misleadingly used by phishing perpetrators includes Paypal, eBay, Washington Mutual Bank, AOL, Citibank, Visa, and Yahoo, among many others. These entities deserve some recourse when their brands are used for criminal and abusive ends.

A violator of this law would be subject both to criminal penalty and civil penalty, providing an effective deterrent to these activities. The bill would define an action subject to civil penalty as a one in which the same or a similar action was conducted, regardless of how many times the action was made. This would allow for a single $100,000 penalty for a set of fraudulent e-mails sent to a group of recipients, a reasonable penalty for such an action.

The criminal justice impact for the bill does not anticipate a significant impact on state correctional facilities. The fiscal note does not anticipate that the bill would require additional resources for the Attorney General's Office to enforce the civil penalties.

OPPONENTS SAY:

Although phishing is a problem, HB 1098 is unnecessary because phishing schemes already violate a host of federal criminal statutes. Depending on the execution of the scheme, participants in phishing could be violating identity theft, wire fraud, credit card fraud, bank fraud, computer fraud, or the recently enacted CAN-SPAM Act, not to mention existing state laws against fraud and identity theft. The federal criminal offenses all carry

substantial penalties ranging as high as 15 to 30 years in prison and $250,000 in fines. The U.S. Justice Department successfully has prosecuted a number of criminal cases involving phishing and can be expected to continue such prosecution in the future.

Any offense that could send more offenders to state correctional facilities should be carefully scrutinized. Current projections estimate that the state will run out of space in state correctional facilities some time this summer, and HB 1098 could exacerbate this situation. State jail and prison facilities should be reserved for violent or repeat offenders and lower level, non-violent property offenders might best be handled on the local level.

OTHER OPPONENTS SAY:

To protect First Amendment concerns, HB 1098 should be amended to ensure that parody Web sites and political speech conducted via the Internet could not be prosecuted as violations under this act.

NOTES:

The committee amendment would lower the civil penalty for violating the bill's provisions from $500,000 in the original bill to $100,000.