COMMENTS

LATE TESTIMONY

TESTIMONY OF
THE DEPARTMENT OF THE ATTORNEY GENERAL
TWENTY-SIXTH LEGISLATURE, 2012

ON THE FOLLOWING MEASURE:
H.B. NO. 1788, H.D. 1, RELATING TO COMPUTER CRIME.

BEFORE THE:

SENATE COMMITTEE ON JUDICIARY AND LABOR

DATE: Thursday, March 27, 2012 **TIME:** 10:30 a.m.

LOCATION: State Capitol, Room 016

TESTIFIER(S): David M. Louie, Attorney General, or
Lance M. Goto, Deputy Attorney General

Chair Hee and Members of the Committee:

The Department of the Attorney General (the "Department") appreciates the intent of this bill, but has concerns and recommends amendments.

The purpose of this bill is to address the problem of computer crime by increasing the grades of offense both for computer fraud and unauthorized computer access offenses, incorporating phishing and the use of spyware into those same offenses, and limiting those offenses to conduct that involves accessing a computer or computer system to obtain identifying information.

The bill creates the new offense of computer fraud in the third degree and defines it as follows:

> A person commits the offense of computer fraud in the third degree if the person knowingly accesses a computer, computer system, or computer network, including by phishing or the use of spyware to obtain identifying information, with the intent to commit the offense of theft in the third or fourth degree.

The bill adds similar wording to the other offenses being amended. The bill adds the phrase, "including by phishing or the use of spyware," to all of the computer fraud and unauthorized computer access offenses. The bill also greatly limits the application of these offenses by requiring as an element of each of the offenses that the offender "obtain identifying information."

IDENTIFYING INFORMATION

The bill defines "identifying information" as personal types of information, such as a social security number, driver's license number, bank account number, credit card number, personal identification number, or account passwords.

The Department must oppose the provisions in this bill that limit the application of the computer fraud and unauthorized computer access offenses by requiring as an element of each of the offenses that the offender "obtain identifying information." These provisions effectively make these offenses apply to few acts of computer crime. Computer fraud generally involves accessing or using a computer to commit theft. The bill, as drafted, results in limiting the computer fraud offenses to situations in which a person accesses a computer to obtain identifying information, with intent to commit theft. In many situations, though, computer fraud does not involve an offender trying to access personal identifying information to commit the theft.

As noted, this bill also limits the offenses of unauthorized computer access to situations in which a person accesses a computer or computer system without authorization to obtain identifying information. The current unauthorized computer access laws prohibit a person from accessing a computer or computer system without authorization to obtain any information. Section 708-890, Hawaii Revised Statutes (HRS), provides that "obtain information" includes but is not limited to the "mere observation of the data." It defines "data" as "information, facts, concepts, software, or instructions prepared for use in a computer, computer system, or computer network." This means that our laws currently protect many kinds of data, not just personal identifying information. This bill will limit the application of our laws and leave large amounts of data and information with less protection than they currently enjoy.

PHISHING OR THE USE OF SPYWARE

The bill adds the phrase, "including by phishing or the use of spyware," to all of the computer fraud and unauthorized computer access offenses. As to these offenses, this bill requires that a person access a computer, computer system, or computer network, "including by phishing or the use of spyware." This new wording is unnecessary, however, because there are many ways that a person may access a computer or computer system. The use of spyware is just one of the many ways to achieve that access, and is already covered under our existing law.

Additionally, phishing is not a means to access a computer or computer system. As defined in the bill itself, "phishing" means "to solicit, request, or take any action to induce a person to provide identifying information." Phishing does not involve accessing a computer to obtain information. It involves inducing a person to provide the information. The bill's use of the term "phishing" as a means of access is therefore somewhat misplaced.

ACCESSING A COMPUTER TO COMMIT OTHER CRIMES, NOT FRAUD

In section 3 of the bill, the offense of computer fraud in the first degree is redefined to include accessing a computer or computer system, with the intent to facilitate the commission of a number of crimes such as murder, kidnapping, extortion, criminal property damage, escape, bribery, or riot. This prohibited conduct does not involve any fraud, and should not be classified as computer fraud. The prohibited conduct may be more appropriate in section 708-893, HRS, use of a computer in the commission of a separate crime.

CONCLUSION

For the foregoing reasons, the Department recommends the removal of the provisions that limit the application of the computer fraud and unauthorized computer access offenses by requiring as an element of each of the offenses that the offender, "obtain identifying information."

The Department recommends the removal of the phrase, "including by phishing or the use of spyware," from all of the computer fraud and unauthorized computer access offenses in the bill.

The Department also recommends the removal of the amendment to the offense of computer fraud in the first degree that attempts to add murder, kidnapping and the other non-fraud-related offenses.

To facilitate these recommendations, the Department has worked closely with the Office of the Prosecuting Attorney, City and County of Honolulu, to create a proposed S.D. 1 that would incorporate our recommendations. Please see the draft attached to this testimony.

We respectfully recommend that the Committee make the suggested amendments.

HOUSE OF REPRESENTATIVES
TWENTY-SIXTH LEGISLATURE, 2012
STATE OF HAWAII

H.B. NO. 1788 H.D. 1 Proposed S.D. 1

A BILL FOR AN ACT

RELATING TO COMPUTER CRIME.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. Chapter 708, Hawaii Revised Statutes, is amended by adding a new section to part IX to be appropriately designated and to read as follows:

"§708- **Computer fraud in the third degree.** (1) A person commits the offense of computer fraud in the third degree if the person knowingly accesses a computer, computer system, or computer network, with the intent to commit the offense of theft in the third or fourth degree.

(2) Computer fraud in the third degree is a class C felony."

SECTION 2. Section 708-891, Hawaii Revised Statutes, is amended to read as follows:

"[~~,~~]§708-891[~~,~~] **Computer fraud in the first degree.** (1) A person commits the offense of computer fraud in the first degree if the person knowingly[~~, and with intent to defraud, accesses a computer without authorization and, by means of such conduct, obtains or exerts control over the property of another.~~

~~(2) In a prosecution for computer fraud in the first degree, it is a defense that the object of the fraud and the property obtained consists only of the use of the computer and the value of such use is not more than $300 in any one-year period.~~] accesses a computer, computer system, or computer network, with the intent to commit the offense of theft in the first degree.

[~~(3)~~] (2) Computer fraud in the first degree is a class [~~B~~] A felony."

SECTION 3. Section 708-891.5, Hawaii Revised Statutes, is amended to read as follows:

"**[~~+~~]§708-891.5[~~+~~] Computer fraud in the second degree.** (1) A person commits the offense of computer fraud in the second degree if the person knowingly[~~, and with the intent to defraud, transfers, or otherwise disposes of, to another, or obtains control of, with the intent to transfer or dispose of, any password or similar information through which a computer, computer system, or computer network may accessed.~~] accesses a computer, computer system, or computer network, with the intent to commit the offense of theft in the second degree.

(2) Computer fraud in the second degree is a class [~~C~~] B felony."

SECTION 4. Section 708-895.5, Hawaii Revised Statutes, is amended to read as follows:

"[~~§~~]§708-895.5[~~§~~] **Unauthorized computer access in the first degree.** (1) A person commits the offense of unauthorized computer access in the first degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby obtains information, and:

(a) The offense was committed for the purpose of commercial or private financial gain;

(b) The offense was committed in furtherance of any other crime;

(c) The value of the information obtained exceeds [~~$5,000;~~] $20,000; or

(d) The information has been determined by statute or rule of court to require protection against unauthorized disclosure.

(2) Unauthorized computer access in the first degree is a class [~~B~~] A felony."

SECTION 5. Section 708-895.6, Hawaii Revised Statutes, is amended to read as follows:

"[~~§~~]§708-895.6[~~§~~] **Unauthorized computer access in the second degree.** (1) A person commits the offense of unauthorized computer access in the second degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby obtains information.

(2) Unauthorized computer access in the second degree is a class [~~C~~] B felony."

SECTION 6. Section 708-895.7, Hawaii Revised Statutes, is amended to read as follows:

"[~~[~~]§708-895.7[~~]~~] **Unauthorized computer access in the third degree.** (1) A person commits the offense of unauthorized computer access in the third degree if the person knowingly accesses a computer, computer system, or computer network without authorization.

(2) Unauthorized computer access in the third degree is a [~~misdemeanor.~~] class C felony."

SECTION 7. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 8. Statutory material to be repealed is bracketed and stricken. New statutory material is underscored.

SECTION 9. This Act shall take effect upon its approval.

Report Title:
Computer Crime

Description:
Creates a third degree of computer fraud. Clarifies and increases penalties for computer fraud in the second degree and first degree. Increases penalties for third, second and first degree unauthorized computer access, and increases the monetary threshold for first degree unauthorized computer access to $20,000. Effective January 7, 2059. (Proposed SD1)

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.

DEPARTMENT OF THE PROSECUTING ATTORNEY
CITY AND COUNTY OF HONOLULU

ALII PLACE
1060 RICHARDS STREET • HONOLULU, HAWAII 96813
PHONE: (808) 547-7400 • FAX: (808) 547-7515

KEITH M. KANESHIRO
PROSECUTING ATTORNEY

ARMINA A. CHING
FIRST DEPUTY PROSECUTING ATTORNEY

COMMENTS

THE HONORABLE CLAYTON HEE, CHAIR
SENATE COMMITTEE ON JUDICIARY AND LABOR
Twenty-sixth State Legislature
Regular Session of 2012
State of Hawai`i

March 27, 2012

RE: H.B. 1788, H.D. 1; RELATING TO COMPUTER CRIME.

AMENDED WRITTEN TESTIMONY

Chair Hee, Vice Chair Shimabukuro and members of the Senate Committee on Judiciary and Labor, the Department of the Prosecuting Attorney, City and County of Honolulu, submits the following testimony in support of House Bill 1788, House Draft 1. Attached, please see the Department's Proposed Senate Draft 1, for your reference and consideration. Proposed Senate Draft 1 was generated to address concerns recently expressed by the Department of the Attorney General.

Proposed Senate Draft 1 removes the language relating to spyware and phishing. However, those methods of "access" would still fall within the scope of the proposed law and would still be prosecuted; they just wouldn't be singled out as methods of access. The Department of the Prosecuting Attorney feels that it is unnecessary to identify those two forms of access to the exclusion of the many other forms of access that suspects use to perpetrate computer fraud and unauthorized access crimes.

The Department agrees with the crux of H.B. 1788, H.D. 1, which would update Hawai'i's computer fraud statutes by adding language similar to Hawai'i's identity theft statutes. Such updates would better address the realities of modern cybercrime, and serve as a more effective tool for enforcement and prosecution of computer fraud offenses.

As currently written, Hawai'i's computer fraud statutes are too narrow to address most activities that are typically thought of as "computer fraud." For example, first-degree computer fraud requires proof that an offender accessed a computer without authorization to obtain or exert control over the property of another. However, most (would-be) computer fraud offenders use their own computer (i.e. with authorization) to carry out offenses, such as online auction fraud,

advance fee scams, counterfeit check scams, phishing and e-mail scams. The language in H.B. 1788, H.D. 1, would fill this gap in the law, using familiar terms from our identity theft statutes.

Similarly, second-degree computer fraud is currently too narrow to effectively prevent or prosecute most types of computer fraud, as it is limited to the misuse of passwords – and that's it. This does not reflect current patterns and schemes used by online fraudsters. The proposed amendments in H.B. 1788, H.D. 1, regarding second- and third-degree computer fraud, would be much more effective and more accurately reflect the realities of modern-day cybercrime.

Similarly, Hawai'i's statutes regarding unauthorized access to computer do not currently reflect the dangers posed by this type of crime. All of us are familiar with the widespread and far-reaching effects that unauthorized computer access can have our society. In 2010, a computer security breach of the University of Hawaii parking garage system affected more than 53,000 people, potentially exposing approximately 41,000 social security numbers and 200 credit card numbers to misuse. Across the country, even larger organizations, such as the Sony Play Station Group, Citigroup, the United States Senate, the C.I.A., and the Arizona State government, have found themselves similarly compromised.

As society becomes increasingly reliant on the Internet for the storage and transfer of our most valuable and confidential information, it becomes increasingly tempting for would-be "hackers" to access our computer networks and information systems without authorization. Moreover, growing Internet connectivity and the proliferation of mobile devices such as tablets and smartphones--combined with the modern ease of creating or obtaining malware--make it possible for practically anyone, anywhere, to engage in online criminal activity at any time.

Even more alarming, we also know that organized criminal groups are increasingly turning to the Internet to commit crimes. They have figured out that the Internet provides anonymity, making it difficult for law enforcement to trace or attribute activity to a particular suspect; they also know that there are a lot of rich targets on the Internet.

Stricter penalties for unauthorized computer access will not only present a stronger deterrent for unauthorized computer access, but also emphasize to the public and would-be offenders that these types of activities will be treated with tougher penalties.

For the reasons noted above, the Department of the Prosecuting Attorney of the City and County of Honolulu supports House Bill 1788, House Draft 1. Thank for you the opportunity to testify on this matter.

HOUSE OF REPRESENTATIVES
TWENTY-SIXTH LEGISLATURE, 2012
STATE OF HAWAII

H.B. NO. 1788 H.D. 1 Proposed S.D. 1

A BILL FOR AN ACT

RELATING TO COMPUTER CRIME.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. Chapter 708, Hawaii Revised Statutes, is amended by adding a new section to part IX to be appropriately designated and to read as follows:

"§708- **Computer fraud in the third degree.** (1) A person commits the offense of computer fraud in the third degree if the person knowingly accesses a computer, computer system, or computer network, with the intent to commit the offense of theft in the third or fourth degree.

(2) Computer fraud in the third degree is a class C felony."

SECTION 2. Section 708-891, Hawaii Revised Statutes, is amended to read as follows:

"[~~[~~]§708-891[~~]~~] **Computer fraud in the first degree.** (1) A person commits the offense of computer fraud in the first degree if the person knowingly[~~, and with intent to defraud, accesses a computer without authorization and, by means of such conduct, obtains or exerts control over the property of another.~~

~~(2) In a prosecution for computer fraud in the first degree, it is a defense that the object of the fraud and the property obtained consists only of the use of the computer and the value of such use is not more than $300 in any one year period.~~] accesses a computer, computer system, or computer network, with the intent to commit the offense of theft in the first degree.

[~~(3)~~] (2) Computer fraud in the first degree is a class [~~B~~] A felony."

SECTION 3. Section 708-891.5, Hawaii Revised Statutes, is amended to read as follows:

"[~~†~~]§708-891.5[~~†~~] **Computer fraud in the second degree.** (1) A person commits the offense of computer fraud in the second degree if the person knowingly[~~, and with the intent to defraud, transfers, or otherwise disposes of, to another, or obtains control of, with the intent to transfer or dispose of, any password or similar information through which a computer, computer system, or computer network may accessed.~~] accesses a computer, computer system, or computer network, with the intent to commit the offense of theft in the second degree.

(2) Computer fraud in the second degree is a class [~~C~~] B felony."

SECTION 4. Section 708-895.5, Hawaii Revised Statutes, is amended to read as follows:

"[~~†~~]§708-895.5[~~†~~] **Unauthorized computer access in the first degree.** (1) A person commits the offense of unauthorized computer access in the first degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby obtains information, and:

(a) The offense was committed for the purpose of commercial or private financial gain;

(b) The offense was committed in furtherance of any other crime;

(c) The value of the information obtained exceeds [~~$5,000;~~] $20,000; or

(d) The information has been determined by statute or rule of court to require protection against unauthorized disclosure.

(2) Unauthorized computer access in the first degree is a class [B] A felony."

SECTION 5. Section 708-895.6, Hawaii Revised Statutes, is amended to read as follows:

"[~~†~~]§708-895.6[~~†~~] **Unauthorized computer access in the second degree.** (1) A person commits the offense of unauthorized computer access in the second degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby obtains information.

(2) Unauthorized computer access in the second degree is a class [~~C~~] B felony."

SECTION 6. Section 708-895.7, Hawaii Revised Statutes, is amended to read as follows:

"[~~1~~]§708-895.7[~~1~~] **Unauthorized computer access in the third degree.** (1) A person commits the offense of unauthorized computer access in the third degree if the person knowingly accesses a computer, computer system, or computer network without authorization.

(2) Unauthorized computer access in the third degree is a [~~misdemeanor.~~] class C felony."

SECTION 7. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 8. Statutory material to be repealed is bracketed and stricken. New statutory material is underscored.

SECTION 9. This Act shall take effect upon its approval.

Report Title:
Computer Crime

Description:
Creates a third degree of computer fraud. Clarifies and increases penalties for computer fraud in the second degree and first degree. Increases penalties for third, second and first degree unauthorized computer access, and increases the monetary threshold for first degree unauthorized computer access to $20,000. Effective January 7, 2059. (Proposed SD1)

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.

COMMENTS

LATE TESTIMONY

Testimony before the Senate Committee on Judiciary and Labor

H.B. 1788, H.D. 1 -- Relating to Computer Crime

Tuesday March 27, 2012
10:30 am, Conference Room 016

By Thomas Overman
Information Assurance Manager
Hawaiian Electric Company, Inc.

Chair Hee, Vice-Chair Shimabukuro and Members of the Committee:

My name is Thomas Overman. I am the Information Assurance Manager for Hawaiian Electric Company. I am testifying on behalf of Hawaiian Electric Company and its subsidiary utilities, Maui Electric Company and Hawaii Electric Light Company.

We support the majority of content in H.B. 1788, H.D. 1, which seeks to strengthen and clarify Chapter 708-890, Hawaii Revised Statutes, but strongly recommend two changes to clarify the legislation. The protection of Personal Identifying Information is clearly in the best interests of everyone. In addition, clarity in the legislative language is critical for any company to be able to implement policies, procedures and systems to protect such information. There are two areas where we strongly encourage modification of the proposed bill.

1) As currently written, the definition of "identifying information" in Section 2 of the proposed legislation does not require correlation in order to require protection. Thus, as written, a Social Security Number (SSN) or customer number out of context, or a seemingly random nine digit number which happens to be someone's SSN, would require protection, even if not correlated with the person's name. To ensure clarity and afford the protections we all desire, we strongly recommend this definition on page 2, line 7 be revised as follows:

"Identifying information" means ~~a person's~~ the correlation of two or more items from the list below, or the correlation of a person's last name with any of the items below:"

2) Also under the definition of "identifying information" on page 2, we agree with and fully support the inclusion of items 1 through 8 on this list. However, item 9, would be impossible to implement. The phrase "any other piece of information" is too broad to be actionable by agencies or companies. This item 9 is a catch-all that nullifies the value of the preceding 8 items, leaving it to the discretion of the reader to determine what is and what is not "identifying information." We therefore strongly recommend item 9 be stricken from the proposed definition of "identifying information."

An alternative path to items 1 & 2 above would be to delete the definition of "Identifying Information" in its entirety. Doing so will help clarify what protections are needed by businesses, and will have the added benefit of avoiding potential conflicts between this legislation and the definition of "Protected Information" in Chapter 487R HRS.

We strongly support the intent of the legislation in clarifying computer crimes and in protecting personal identifying information. We feel that the changes recommended above will make the legislation, and any resulting regulations, much more clear and unambiguous.

Thank you for the opportunity to testify.

From: mailinglist@capitol.hawaii.gov
Sent: Monday, March 26, 2012 11:21 AM
To: JDLTestimony
Cc: breaking-the-silence@hotmail.com
Subject: Testimony for HB1788 on 3/27/2012 10:30:00 AM

Testimony for JDL 3/27/2012 10:30:00 AM HB1788

Conference room: 016
Testifier position: Support
Testifier will be present: No
Submitted by: Dara Carlin, M.A.
Organization: Individual
E-mail: breaking-the-silence@hotmail.com Submitted on: 3/26/2012

Comments:
Good Morning Senators ~

Please support this measure against cyber-crime as victim-survivors of domestic violence are at increased risk for such crimes.

Thank you most sincerely for this opportunity to provide testimony.

Respectfully,

Dara Carlin, M.A.
Domestic Violence Survivor Advocate