DISCLAIMER

Electronic versions of the exhibits in these minutes may not be complete.

This information is supplied as an informational service only and should not be relied upon as an official record.

Original exhibits are on file at the Legislative Counsel Bureau Research Library in Carson City.

Contact the Library at (775) 684-6827 or library@lcb.state.nv.us.

Senate Bill 297: Identity Theft
Senator Valerie Wiener
March 31, 2003

Mr. Chairman and members of the Committee, for the record, I am State Senator Valerie Wiener, representing Clark County, District 3. Today I appear before you to urge your support for Senate Bill 297, which addresses identity theft.

This relatively new crime has produced great fear in people who want to be able to place faith in their credit or debit card transactions. Yet, with technology–and the abuse of it by unscrupulous people–millions of Americans are at risk when they use these convenient instruments of commerce.

Let's go to the bill itself to see what I propose as substantial protections against identity theft.

To help you understand primary components of the bill, you will find key definitions, necessary to the enforcement of the legislation. Section 3 defines "payment card;" Section 4 defines "re-encoder;" and Section 5 defines "scanning device."

Section 6 prohibits a person from using a scanning devise or a re-encoder WITHOUT the permission of the authorized user of the payment card AND with the intent to defraud the authorized user, the issuer of the card, or anyone else. A person who violates these provisions is guilty of a B felony, and would serve from one to 20 years in prison and could be fined up to $100,000.

In addition, the court shall order the violator to pay restitution, including attorney's fees and the costs required to repair each victim's credit history or rating AND satisfy the debt, lien, or other obligation incurred by each victim.

Section 7 prohibits the possession of a scanning device or re-encoder with the INTENT to use for an unlawful purpose. Any violation of this is a C felony.

Section 8 protects those people who do NOT have intent to defraud or commit an unlawful act, but possess or use a scanning device or re-encoder in the ordinary course of business or employment.

Section 9 deals with prosecution. The state is not required to establish–and it is not a defense that: 1) an accessory has not been convicted, apprehended, or identified OR 2) some of the acts constituting elements of the crime did NOT occur in this state OR, where such acts did occur, they were not a crime or elements of a crime.

Section 11 defines "document;" Section 12 extensively defines "personal identifying information;" Section 13 defines "public body;" Section 14 defines "public employee;" Section 15 defines "public officer."

Section 16 helps plug a statutory oversight by allowing for the prosecution for the identity theft of a person . . . living or DEAD. Current law does not address the theft of a deceased's name or identity.

Section 17 addresses situations where a public officer or public employee KNOWINGLY obtains another person's personal identifying information from any source or resource used by a public body to collect or otherwise handle personal identifying information AND USES that information to HARM that person, or for ANY UNLAWFUL PURPOSE. These purposes include such activities as obtaining credit, a good, or service in that person's name.

Any public officer of public employee who violates this will be guilty of a B felony, with a five-to-20-year sentence and up to $100,000 fine. You can compare the minimum time of 5 years for a public officer of employee with the sanctions in Section 6 for persons using scanning devices or re-encoders. Section 6 violators would be guilty of a B felony, as well, but their minimum time is one year. I asked for a stiffer minimum for public officers or employees, because they hold the public trust AND we do not ordinarily have the option of saying "no" to their requests for this information.

As with other offenders, public officers or employees will be held financially accountable for repairing the credit history of their victims, as well as satisfying the debts, liens, or other obligations incurred through the identity theft.

In addition, if a public employee or officer obtains personal identifying information AND possesses, sells, or transfers this information to establish a false status, occupation, membership, license, or identity for himself or another person, he will be guilty of a C felony. If a public employee or officer knowingly aids another public employee or officer in violating any of these provisions, he, too, is guilty of a C felony. Please take note that law enforcement is not prohibited from using personal identifying information if this is related to a lawful discharge of their duties.

Section 18, as in other sections in the bill, states that these provisions do not apply to persons who, without the intent to defraud or commit an unlawful act, possess or use another person's identifying information in the ordinary course of their business or employment. OR . . . they have entered into a financial transaction with the authorized user of a payment card who has agreed to the financial transaction.

In Section 19, the state is not required to establish –and it is not a defense that–an accessory has not been convicted, apprehended, or identified OR that some elements of the crime might have occurred elsewhere or that these same acts might not constitute a crime elsewhere.

Section 22 defines "credit card" and "debit card," and addresses concerns about credit or debit card receipts. This section prohibits the printing on the customer receipt for a credit or debit card . . . of: the expiration date AND the more than the last five digits of the account number.

This applies only to receipts that are electronically printed. It does not apply to receipts that are handwritten or imprinted or copied. If the cash register or printing device (which includes ATM machines) was first put into use before October 1, 2003, this requirement will not apply until January 1, 2006.

Mr. Chairman and members of the committee, identity theft has become one of the most egregious crimes in our country today. People have become fearful of doing business because of their concerns that someone, often unknown to them, might "steal" their identities. Such an identity theft can haunt the victim's ability to do business under his or her name for years to follow. Learned this 2 sessions ago.

I was the unknowing victim of identity theft in October 2001. Fortunately, my credit card company notified me the same day that irregular charges appeared on my credit card. When I returned their call, they told me that they did not process the charge for about $4,600 for "Internet Computer Consulting Services–Overseas." I responded with a big "whew" and a loud "thanks" for their diligence. They followed my appreciation with and explanation that they didn't process the charge because it surpassed my credit line. They then confirmed that they DID process the charge for the same services, the same day, for more than $16,300.

Fortunately, because my credit card company spotted an irregular use of my card, they called me. Fortunately, the same day as the fraudulent charges–and the identity theft I experienced–the credit card company was able to "right the wrong" on my credit card account. I don't know how it was stolen from me, since that particular card is only issued to me, and I only make in-person charges with it. I DO know that, since then, I have been queasy every time I hand over my card.

It is my hope that, for the tens of thousands of people who are concerned about the safety and protection of their identities, Senate Bill 297 will provide some needed assurances.

SB 297 creates substantial penalties for people who steal personal identifying information. Because it is important for us to protect the identities of the people we serve, I urge your support for Senate Bill 297. Thank you.