

Washington's **Law Enforcement Group** against **Identity Theft** (LEGIT)

A statewide group of legislators, police chiefs, sheriff's, prosecutors,
business and financial industry security professionals, and private sector associations,
working to reduce identity theft in Washington.

January 17, 2007

Identity Theft Task Force PO 65410
Federal Trade Commission
Office of the Secretary, Room H-135 (Annex N)
600 Pennsylvania Avenue N.W.
Washington, D C 20580

Re: Federal Identity Theft Task Force Notice for Public Comment

Dear Attorney General Alberto Gonzales, Chairman Deborah Platt Majoras, and
members of the Federal Identity Theft Task Force:

This letter is in response to your request for public comment. I am writing on behalf of Washington State's Law Enforcement Group against Identity Theft (LEGIT), which I chair. This statewide group was initiated by Washington State's Attorney General and is composed of police chiefs and sheriffs, prosecutors, legislators, private industry security professionals, and public and private associations. I am a 20 year veteran prosecutor. I have investigated and prosecuted crimes involving identity theft for more than 10 years, teach police and prosecutor identity theft courses nationally for the National Center for Prosecution of Identity Crimes and the American Prosecutor's Research Institute, and serve on Washington state and national identity theft advisory committees.

I. MAINTAINING SECURITY OF CONSUMER DATA.

Efforts to reduce the ease of access to identity and financial data by increasing security in handling of consumer data are critical to our success in addressing identity theft. Stop the crime before it occurs by making the information central to the crime (a consumer's identity and financial data) harder and riskier to obtain. The federal task force recommendations in this area include a recommendation to the Office of Personnel Management that it "eliminate the gratuitous use of SSNs in human resources forms used by federal agencies." This is an important goal, but does not go far enough. This task force should also recommend that Congress closely regulate and limit collection, storage, handling, display, and uses of federally issued and controlled SSNs by organizations and individuals, whether public or private. The task force touches on this concept in the five additional measures listed as being under consideration.

1. Government Use of SSNs

Reduced government use of SSNs at all levels is an important goal. An employee's SSN should not be printed on his paycheck, pay stub, or most other correspondence between the employer and employee. Employee insurance should not use the employee's SSN as an identification number, nor should employee training courses collect or be tracked by

the employee SSN. One disturbing example of overuse of SSNs by government involves training required of our law enforcement officers as a condition of maintaining FEMA certification. Despite the fact that the officer's employer has the officer's SSN, and can certify to FEMA that the officer is commissioned with the particular law enforcement agency, FEMA apparently insists that the officer place his SSN on the testing form.

2. Comprehensive Record on Private Sector Use of SSNs

While a study of how the private sector collects and uses SSNs would be enlightening, such a study is not a necessary precursor to taking effective action now. Both private and public sector entities should be restricted to collecting and using SSNs for purposes related to reporting to the SSA. Customer SSNs should not be collected and stored by medical providers, renters of videos, or telephone service providers and other businesses.

3. National Data Security Standards

This is an important recommendation. How all entities maintain sensitive consumer information greatly affects the ease with which criminals can obtain access to that information. If this information must be collected, it must be maintained securely, and properly destroyed. As a prosecutor, I have handled several cases of identity theft in which the initial theft of the sensitive identifying personal data occurred because the organization for which the thief worked failed to restrict access to this data on a need to know basis, or at all. Examples include a city employee stealing identity and financial data from employees' personnel files, and medical provider receptionists and others (who had no need for access to identity information) stealing patient name, DOB and SSN. In a case where contract answering service employees stole customer names, dates of birth and SSNs, the information was in the database provided to the answering service, even though this information was not absolutely necessary for the contract employee to perform his duties. Organizations that have best responded to these concerns have instituted internal policies restricting access to personal identity and financial information on a need to know basis; conduct audits to determine compliance with the policies; and discipline employees who fail to comply with the policies.

Both government and private sector entities should be prohibited from displaying identity and financial information in correspondence with employees and consumers. Neither SSNs nor complete account numbers should be printed on correspondence mailed or e-mailed to consumers. According to several reports and anecdotal evidence supplied by law enforcement, mail theft remains among the top sources of identity information obtained by identity thieves. Businesses and government entities alike should be required to establish and maintain secure mail drops for all incoming and outgoing mail for the organization, and to eliminate access to this mail beyond mail handlers and either the postal service or the ultimate recipient of the correspondence.

Disposal of consumer identity and financial data is also an important area in need of improved regulation. Though the federal laws require financial institutions to destroy this data before disposal, and some states, including Washington, require business and government to destroy this data before its disposal, these laws have very limited scope and very low enforcement values. For example, the federal law is limited to financial institutions, and the Washington law has no government enforcement clause.

Finally, a Reuter's article published January 17, 2007, poignantly raises questions about responsible maintenance of consumer identity data. The article, titled, "TJX says system breached, customer data stolen" (by an intrusion into their computer system) states that customer credit and identity information dating back to 2003 was stolen. TJX is not alone in leaving years-old data on computer systems that can be accessed, and hacked, via the internet. A federal task force study in this area would well serve the citizens of this country. The study would seek to identify actual business need for maintaining data accessible to the internet, find ways to reduce the risk, and ultimately balance between those needs and the risks associated with such access.

II. PREVENTING THE MISUSE OF CONSUMER DATA

Beyond restricting access to identity data on a need to know basis, lenders and bankers should be required to verify the credit applicant's identity by reviewing the customer's credit report for, at minimum, a tri-part match of the name, date of birth and SSN on the documents completed by the customer and a credit report obtained from a major credit reporting agency. Too often, lenders eager to do business use only one or two of these identifiers when checking the customer's application, and thus fail to recognize that the applicant is an identity thief. Business loss tax deductions should be denied to those entities that do not verify this tri-part match and subsequently face loss due to identity fraud.

Additionally, though consumer reporting agencies collect and maintain identity and financial data on consumers, they do not create that data, nor does that data "belong" to the CRA in the same way it belongs to the consumer. We refer to the consumer's name, the consumer's date of birth, the consumer's SSN, and the consumer's credit history. Normally the consumer's financial behavior determines the consumer's credit score and ability to obtain employment, rent property, and get credit. But when other individuals commit identity fraud that damages a consumer's credit history and credit score, typically the consumer, and no one else, bears the burden of repairing that damage, or of living with that damage. Consumers need greater authority to prevent misuse of their data in the first place. Consumers should be allowed to place fraud alerts and credit freezes, and to prevent consumer reporting agencies from selling or sharing any data about the consumer, regardless of whether the consumer has been a victim of identity fraud. Many current laws require the consumer to have been a victim of identity fraud before these tools become available. That is akin to closing the barn door after the horse has already escaped.

Some identity theft cases arise from theft of credit offers from the mail. Consumers should be required to "opt in" to receive these offers, rather than having to "opt out" to avoid "pre-approved credit offers," blank checks, and other similar offers of credit.

III. VICTIM RECOVERY

1. Improving Victim Assistance

Your federal task force has considered numerous ways to increase assistance to victims of identity fraud. All are important. A victim of identity theft attempting to recover from

the crime must often enter into an environment that is entirely foreign to that person. He has no prior experience to guide his actions and decisions. He does not automatically know where to turn. Training local law enforcement in these questions, and providing first responders with educational and instructive materials they can hand out to consumer victims would be an important step in assisting victim recovery.

In prosecutor's offices with which I am familiar, victim advocates' duties are generally restricted to assisting victims and families of violent crimes such as homicide, rape, robbery, assault, and domestic violence. Even though studies project that as many as one of every ten American adults will be identity fraud victims in their lifetime, victim advocates usually are not tasked with assisting victims of identity fraud, and rarely have time to take on these additional cases. Victim advocates are not trained in, and frequently are not familiar with the myriad steps an identity theft victim must take on the road to recovery. Though at least one study has reported that victims of repeated identity fraud can face some of the same kinds of emotional trauma as can victims of repeated domestic violence, I know of no formal training that educates victim advocates of this fact and prepares the advocate to assist the victim in coping with this reality. Local police and prosecutors need additional funding and additional victim assistance counselors available to assist victims of identity fraud, even more than nationwide training of victim assistance counselors.

2. Making Identity Theft Victims Whole

In addition to the Federal Identity Theft Task Force recommendation to amend the restitution laws, those who negligently provide credit in a victim's identity, or who negligently dispose of consumer identity and financial information, should also be liable to affected consumers. One Washington state senator is currently drafting legislation that would give a consumer the right to sue and obtain damages and exemplary damages from merchants and lenders who negligently a) provide credit in a consumer's identity, or b) disclose, misplace, or dispose of a consumer's identity and financial data. The anticipated side effect of such a law is increased care by merchants and lenders in their granting of credit, and their storing, handling, and disposal of consumer identity information.

3. National Program Allowing Identity Theft Victims to Obtain an Identification Document for Authentication Purposes.

This is an important goal, and such programs have apparently worked well on a state by state basis. However, this is a "back end" approach to the problem of identity fraud – providing a national identification document only after a citizen has been victimized. A "front end" approach may prove more fruitful. The most common form of photo identity documentation is the state-issued driver's license or identification card. The appearance and security features of those cards vary from state to state. Though many in law enforcement are trained in how to recognize valid identity documents, many others in both government and the private sector are not similarly trained. This increases the ease with which an identity thief can obtain credit, merchandise or other items or services upon presentation of a fraudulent "government issued" identity card. A single national

identity card would go far to eliminate this problem. At the very least, there should be minimum requirements for issuing a driver's license.

Second, when an identity thief identifies himself to police as the citizen whose identity he has assumed, this causes the risk of serious consequences to the identity theft victim, including arrest and imprisonment for crimes committed by an identity thief, but that police have associated with the victim. Beyond a national identity card or document, identity theft victims would be well served by establishing a uniform identity theft flag or entry into a national database used by law enforcement to check detainees for criminal history, warrants and the like. Such an entry will prompt the detaining officer to ask additional questions in an effort to determine the true identity, and thus the true criminal, arrest, and warrant status of the detained person.

4. FTC Identity Fraud Report. The new FTC identity fraud report is another good step in the right direction in assisting identity theft victims. Ongoing FTC efforts to publicize the existence of this affidavit, and to ensure that credit reporting agencies merchants, financial institutions, and the like accept and rely on the report, are also important and worthy activities. Victims almost always need police or incident reports of identity theft before they can obtain long term fraud alerts on their credit reports and, before the victim can obtain records from a transaction between a lender or merchant and an identity thief. For various reasons, many police departments continue to decline to take identity fraud reports from victims. The new FTC identity fraud report might resolve some of this problem, but it likely won't resolve it all. This is because the FTC procedure requires the identity theft victim to, after making the report to the FTC, take the report to their local police agency and obtain a police incident number and police department verification of the report. To the extent that law enforcement agencies decline to take incident reports because of the time required to take the reports, a victim's presentation of a pre-completed FTC report would likely result in the desired result – local PD verification and an incident number. But to the extent that the local PD declines to take the report for other reasons, the FTC report will not resolve the problem. Either identity fraud victims should be able to obtain freezes, fraud alerts, and repair of their credit without being required to produce a police report, or law enforcement should be required to take or verify incident reports of citizens who report that their identities have been compromised in any form, including loss by an organization.

5. Medical Identity Fraud. Victim recovery from medical identity fraud is another critical area for study and enforcement. In medical identity fraud, the criminal obtains medical treatment in the victim's identity. Records of the medical treatment provided to the criminal are added to the victim's medical record. So, for example, if the criminal has his appendix taken out, the victim's medical record shows that the victim had *his* appendix out. Later, if the victim develops appendicitis, physicians wrongly believing that the victim has no appendix may misdiagnose the problem, at great danger to the victim. Victims of medical identity fraud who discover the fraud face extreme difficulty in repairing their medical records. Physicians are understandably reluctant to remove records from a medical file, yet victims must have the records corrected to assure proper medical treatment in the future. The federal identity theft task force would greatly

serve both medical professions and American citizens by establishing clear guidelines for medical identity fraud recovery.

IV. LAW ENFORCEMENT: PROSECUTING AND PUNISHING IDENTITY THIEVES

2. Ability of Law Enforcement to Receive Information From Financial Institutions

This task force consideration focuses primarily on financial institutions. Law enforcement needs records from many types of organizations. Merchants, financial institutions, employers, contractors, and charitable organizations are only a few. Identity thieves are highly mobile, crossing state and even national borders. Financial institutions, other corporations, and other organizations regularly operate on a national and international basis. Yet most law enforcement is local, and has legal authority to compel production of records from these organizations only when the organization is within the orders of the state in which the particular law enforcement agent works, or when those records are physically located within the state. To effectively combat this crime, law enforcement at all levels must have the ability to compel production of records relevant to the investigation, regardless of the location of those records or of the entity holding those records. This law is needed for all entities, not just financial institutions.

Section 609(e) of the Fair Credit Reporting Act requires production of transaction records, but not of all existing evidence relevant to the transaction. This requirement is too narrow. For example, one Washington bank refuses to provide a video recording of a transaction that law enforcement is investigating as an identity theft, and nothing in 609(e) would clearly require the bank to provide this compelling evidence.

Other measures that would improve law enforcement and prosecutor's ability to bring identity thieves to justice include:

- a. Video retention. A significant proportion of financial institutions, merchants and casinos operate video equipment to record financial transactions, including purchases, credit applications, and disbursement of cash. Many casinos in Washington retain these videos for only 7 days; merchants and financial institutions frequently retain these recordings for only 30 days. In a very high proportion of identity theft cases, victims do not learn of their victimization until well beyond these 30 days. Law enforcement's ability to bring identity thieves to justice would be greatly enhanced by a federal law requiring these videos to be maintained for 90 or 180 days.
- b. Video subject focus. Many of those entities that video record financial transactions, focus their video capture on their employee only, and fail to place the camera so it can also capture an image of the customer's face. Federal law requiring that any video recordings of financial transactions include an image of the customer would greatly improve law enforcement's ability to identify and bring identity thieves to justice.
- c. Record holders contact information. Federal law should require that financial institutions, merchants, and others who collect consumer identity information provide and publicize contact information for persons within the organization who

are tasked with assisting law enforcement in obtaining records necessary to the police investigation.

d. Admissibility and legal foundation for records of identity theft. There should be a national law defining business records and allowing for their legal foundation and admissibility in both criminal and civil matters, without the need for an employee of the providing organization to appear in court to identify the records. This would increase effectiveness of law enforcement and prosecution efforts to bring identity thieves to justice while decreasing costs to taxpayers and to the record providing organizations, who often are also victims of identity fraud. The Washington state legislature will consider such a proposal this session. A copy of that proposal, S-0125, is included with this letter.

e. Joint local and federal law enforcement efforts. Greater cooperation between local and federal law enforcement, and between local and federal prosecutors, in the form of task forces, working groups, or otherwise, enhances overall law enforcement efforts. The United State's Attorney's Office for the Western District of Washington, several federal law enforcement agencies, and several Washington state counties have forged strong alliances that have resulted in significant success in law enforcement's efforts to bring identity thieves to justice.

f. Data analysis. Unlike most traditional violent crime, identity theft investigations are paper intensive and require analytical skills that many in traditional law enforcement either do not possess or do not have the time to employ, given their other duties. Effective data collection and analysis is critical successfully bringing identity thieves to justice, particularly those that work in groups. Recognizing this, several law enforcement agencies have obtained funding for data analysts who specifically focus on identifying, obtaining and analyzing the necessary records. Broader national use of this investigative approach, unrestricted by local jurisdictional boundaries, should greatly improve law enforcement's efforts to bring identity thieves to justice.

Thank you for this opportunity to provide comment. I am including with this letter copies of the identity theft related legislation the Washington legislature will consider this session. I can be reached at 206-296-9077 for further discussion of these or related matters.

Sincerely,

Susan K. Storey
Chair,
Washington's Law Enforcement Group against Identity Theft

Senior Deputy Prosecuting Attorney
Fraud Division
King County Prosecutor's Office
500 Fourth Avenue, Room 840
Seattle, WA 98104

BILL REQUEST - CODE REVISER'S OFFICE

BILL REQ. #: S-0125.1/07

ATTY/TYPIST: AI:ads

BRIEF DESCRIPTION: Obtaining records in a criminal investigation.

1 AN ACT Relating to records in a criminal investigation; and adding
2 a new chapter to Title 10 RCW.

3 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

4 NEW SECTION. **Sec. 1.** The legislature finds that many businesses,
5 associations, and organizations providing goods and services to the
6 public, conducting other activity in Washington, or otherwise affecting
7 residents of Washington now operate nationally or globally and often
8 maintain their business records in a location outside the state of
9 Washington. The legislature further finds that bringing persons or
10 organizations committing crimes in Washington to justice is a matter of
11 great public interest because crimes have a significant effect on
12 businesses, associations, and other organizations that conduct business
13 in Washington, as well as on Washington citizens. Crimes result in
14 significant harm and losses to persons, businesses, associations, and
15 other organizations victimized, as well as persons not directly
16 victimized when businesses or others more directly affected by the
17 crimes must raise prices to cover crime losses. The ability of law
18 enforcement and the criminal justice system to effectively perform
19 their duties to the public often depends upon law enforcement agencies,

1 prosecutors, and criminal defense attorneys being able to obtain and
2 use records relevant to crimes that affect Washington's citizens,
3 businesses, associations, organizations, and others who provide goods
4 or services, or conduct other activity in Washington. In the course of
5 fulfilling their duties to the public, law enforcement agencies,
6 prosecutors, and criminal defense attorneys must frequently obtain
7 records from these entities, and be able to use the records in court.
8 The ability to obtain and use these records has an impact on Washington
9 citizens because it affects the ability to enforce Washington's
10 criminal laws and affects the deterrence value arising from criminal
11 prosecution. Effectively combating crime requires laws facilitating
12 and requiring that all those who possess records relevant to a criminal
13 investigation comply with the legal process issued in connection with
14 criminal investigations or litigation.

15 NEW SECTION. **Sec. 2.** The definitions in this section apply
16 throughout this chapter unless the context clearly requires otherwise.

17 (1) "Adverse result" includes one of the following possible
18 consequences:

19 (a) Danger to the life or physical safety of an individual;

20 (b) A flight from prosecution;

21 (c) The destruction of, potential loss of, or tampering with
22 evidence;

23 (d) The intimidation of potential witnesses;

24 (e) Jeopardy to an investigation or undue delay of a trial.

25 (2) "Applicant" means a law enforcement officer, prosecuting
26 attorney, deputy or special deputy prosecuting attorney, or defense
27 attorney who is seeking criminal process under section 3 of this act.

28 (3) "Criminal process" means a search warrant or legal process
29 issued pursuant to RCW 10.79.015 and CrR 2.3; any process issued
30 pursuant to chapter 9.73, 9A.82, 10.27, or 10.29 RCW; and any other
31 legal process signed by a judge of the superior court and issued in a
32 criminal matter which allows the search for or commands production of
33 records that are in the actual or constructive possession of the
34 recipient, regardless of whether the recipient or the records are
35 physically located within the state.

36 (4) "Defense attorney" means an attorney of record for a person

1 charged with a crime when the attorney is seeking the issuance of
2 criminal process for the defense of the criminal case.

3 (5) "Properly served" means delivery by hand or in a manner
4 reasonably allowing for proof of delivery if delivered by United States
5 mail, overnight delivery service, or facsimile to the recipient
6 addressee of criminal process.

7 (6) "Recipient" means a person, as defined in RCW 9A.04.110, or a
8 business, as defined in RCW 5.45.010, upon whom criminal process issued
9 under this chapter is properly served.

10 NEW SECTION. **Sec. 3.** The following shall apply to any criminal
11 process allowing for search of or commanding production of records that
12 are in the actual or constructive possession of a recipient who
13 receives service outside Washington, regardless of whether the
14 recipient or the records are physically located within the state.

15 (1) When properly served with criminal process issued under this
16 section, the recipient shall provide the applicant all records sought
17 pursuant to the criminal process. The records shall be produced within
18 twenty business days of receipt of the criminal process, unless the
19 process requires earlier production. An applicant may consent to a
20 recipient's request for additional time to comply with the criminal
21 process.

22 (2) Criminal process issued under this section must contain the
23 following language in bold type on the first page of the document:
24 "This [warrant, subpoena, order] is issued pursuant to RCW [insert
25 citation to this statute]. A response is due within twenty business
26 days of receipt, unless a shorter time is stated herein, or the
27 applicant consents to a recipient's request for additional time to
28 comply."

29 (3) If the judge finds that failure to produce records within
30 twenty business days would cause an adverse result, the criminal
31 process may require production of records within less than twenty
32 business days. A court may reasonably extend the time required for
33 production of the records upon finding that the recipient has shown
34 good cause for that extension and that an extension of time would not
35 cause an adverse result.

36 (4) When properly served with criminal process issued under this
37 section, a recipient who seeks to quash the criminal process must seek

1 relief from the court where the criminal process was issued, within the
2 time originally required for production of records. The court shall
3 hear and decide the motion no later than five court days after the
4 motion is filed. An applicant's consent, under subsection (1) of this
5 section, to a recipient's request for additional time to comply with
6 the criminal process does not extend the date by which a recipient must
7 seek the relief designated in this section.

8 NEW SECTION. **Sec. 4.** (1) Upon written request from the applicant,
9 or if ordered by the court, the recipient of criminal process shall
10 verify the authenticity of records that it produces by providing an
11 affidavit, declaration, or certification that complies with subsection
12 (2) of this section and providing contact information for the person
13 completing the affidavit, declaration, or certification. Records
14 produced in compliance with this section are admissible as evidence
15 under this section.

16 (2) A record provided by a recipient of criminal process under this
17 section shall not be excluded as hearsay evidence or for lack of
18 foundation or authentication if accompanied by an affidavit,
19 declaration, or certification by its record custodian or other
20 qualified person that attests to the following:

21 (a) The record was made at or near the time of the act, condition,
22 or event set forth in the record by, or from information transmitted
23 by, a person with knowledge of those matters;

24 (b) The record was made in the regular course of business;

25 (c) States the identity of the record and sets forth the mode of
26 its preparation; and

27 (d) If such record is not the original, it is a duplicate that
28 accurately reproduces the original.

29 (3) No evidence in the records in the form of opinion or diagnosis
30 is admissible under this section unless the opinion or diagnosis would
31 otherwise be admissible.

32 (4) A party intending to offer a record into evidence under this
33 section must provide written notice of that intention to all adverse
34 parties, and must make the record and affidavit, declaration, or
35 certification available for inspection sufficiently in advance of their
36 offer into evidence to provide an adverse party with a fair opportunity
37 to challenge them. A motion opposing admission in evidence of the

1 record shall be made and determined by the court before trial and with
2 sufficient time to allow the party offering the record time, if the
3 motion is granted, to produce the custodian or records or other
4 qualified person at trial, without creating hardship on the party or on
5 the custodian or other qualified person. A motion opposing
6 introduction of the records must be based on one or more of the
7 following reasons: (a) Failure to comply with this section; (b)
8 failure of the records, as proposed to be offered, to be substantially
9 understood without further explanation and no other witness is
10 available to explain them; or (c) admission of the records would
11 violate ER 403.

12 (5) Failure by a party to timely file a motion under subsection (4)
13 of this section shall constitute a waiver of objection to admission of
14 the evidence, but the court for good cause shown may grant relief from
15 the waiver. When the court grants relief from the waiver, and
16 thereafter determines the custodian of records shall appear, a
17 continuance of the trial may be granted to provide the proponent of the
18 records sufficient time to arrange for the necessary witness to appear.

19 (6) Nothing in this section precludes either party from calling the
20 custodian of record of the record or other witness to testify regarding
21 the record.

22 NEW SECTION. **Sec. 5.** A Washington recipient, when served with
23 process that was issued by or in another state that, if it were issued
24 in Washington, would be criminal process, shall comply with that
25 process as if that warrant or other qualifying legal process had been
26 issued by a Washington court.

27 NEW SECTION. **Sec. 6.** A recipient of criminal process or process
28 under sections 2 and 5 of this act, and any other person that responds
29 to such process is immune from civil liability for complying with the
30 process, and for any failure to provide notice of any disclosure to the
31 person who is the subject of or identified in the disclosure.

32 NEW SECTION. **Sec. 7.** A judge of the superior court may issue any
33 criminal process to any recipient at any address, within or without the
34 state, for any matter over which the court has criminal jurisdiction

1 pursuant to RCW 9A.04.030. This provision does not limit a court's
2 authority to issue warrants or legal process under other provisions of
3 state law.

4 NEW SECTION. **Sec. 8.** Sections 1 through 7 of this act constitute
5 a new chapter in Title 10 RCW.

--- END ---

BILL REQUEST - CODE REVISER'S OFFICE

BILL REQ. #: S-0126.3/07 3rd draft

ATTY/TYPIST: AI:seg

BRIEF DESCRIPTION: Changing identity theft provisions.

1 AN ACT Relating to identity theft; amending RCW 9.35.001, 9.35.020,
2 and 46.20.0921; creating a new section; and prescribing penalties.

3 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

4 NEW SECTION. **Sec. 1.** The legislature enacts this act to expressly
5 reject the interpretation of *State v. Leyda*, 157 Wn.2d 335, 138P.3d 610
6 (2006), which holds that the unit of prosecution in identity theft is
7 any one act of either knowingly obtaining, possessing, using, or
8 transferring a single piece of another's identification or financial
9 information, including all subsequent proscribed conduct with that
10 single piece of identification or financial information, when the acts
11 are taken with the requisite intent. The legislature finds that
12 proportionality of punishment requires the need for charging and
13 punishing for obtaining, using, possessing, or transferring any
14 individual person's identification or financial information, with the
15 requisite intent. The legislature specifically intends that each
16 individual who obtains, possesses, uses, or transfers any individual
17 person's identification or financial information, with the requisite
18 intent, be classified separately and punished separately as provided in
19 chapter 9.94A RCW.

1 **Sec. 2.** RCW 9.35.001 and 1999 c 368 s 1 are each amended to read
2 as follows:

3 The legislature finds that means of identification and financial
4 information ~~((is))~~ are personal and sensitive information such that if
5 unlawfully obtained, possessed, used, or transferred by others may
6 ~~((do))~~ result in significant harm to a person's privacy, financial
7 security, and other interests. The legislature finds that unscrupulous
8 persons find ever more clever ways, including identity theft, to
9 improperly obtain ~~((and))~~, possess, use, and transfer another person's
10 means of identification or financial information. The legislature
11 intends to penalize ~~((unscrupulous people))~~ for each unlawful act of
12 improperly obtaining, possessing, using, or transferring means of
13 identification or financial information of an individual person. The
14 unit of prosecution for identity theft by use of a means of
15 identification or financial information is each individual unlawful use
16 of any one person's means of identification or financial information.
17 Unlawfully obtaining, possessing, or transferring each means of
18 identification or financial information of any individual person, with
19 the requisite intent, is a separate unit of prosecution for each victim
20 and for each act of obtaining, possessing, or transferring of the
21 individual person's means of identification or financial information.

22 **Sec. 3.** RCW 9.35.020 and 2004 c 273 s 2 are each amended to read
23 as follows:

24 (1) No person may knowingly obtain, possess, use, or transfer a
25 means of identification or financial information of another person,
26 living or dead, with the intent to commit, or to aid or abet, any
27 crime.

28 (2) Violation of this section is identity theft in the first degree
29 when the accused, a conspirator, or an accomplice ~~((uses the victim's~~
30 ~~means of identification or financial information and))~~:

31 (a) Obtains ~~((an aggregate total of))~~ credit, money, goods,
32 services, or anything else of value in excess of one thousand five
33 hundred dollars in value ~~((shall constitute identity theft in the first~~
34 ~~degree))~~; or

35 (b) Acts with intent to transfer the means of identification or
36 financial information to another person; or

1 (c) Transfers the means of identification or financial information
2 to a third person; or

3 (d) Uses the means of identification or financial information to
4 manufacture, or with intent to manufacture, any false means of
5 identification, financial documents, accounts, or records for transfer
6 to or use by any other person; or

7 (e) Obtains, possesses, transfers, or uses the means of
8 identification or financial information through use of the actor's
9 position as a "trusted person" as defined in RCW 9A.68.060; or

10 (f) Violates RCW 46.20.0921(3)(a); or

11 (g) During a contact with a law enforcement officer, uses the means
12 of identification or financial information as a form of identification.
13 Identity theft in the first degree is a class B felony punishable
14 according to chapter 9A.20 RCW.

15 ~~(3) ((Violation of this section when the accused or an accomplice~~
16 ~~uses the victim's means of identification or financial information and~~
17 ~~obtains an aggregate total of credit, money, goods, services, or~~
18 ~~anything else of value that is less than one thousand five hundred~~
19 ~~dollars in value, or when no credit, money, goods, services, or~~
20 ~~anything of value is obtained shall constitute identity theft in the~~
21 ~~second degree.)) A person is guilty of identity theft in the second
22 degree when he or she violates subsection (1) of this section under
23 circumstances not amounting to identity theft in the first degree.
24 Identity theft in the second degree is a class C felony punishable
25 according to chapter 9A.20 RCW.~~

26 (4) Except as provided in subsection (5) of this section, each
27 crime prosecuted under this section shall be punished separately under
28 chapter 9.94A RCW, unless it is the same criminal conduct as any other
29 crime, under RCW 9.94A.589.

30 (5) Whenever any series of transactions involving a single person's
31 means of identification or financial information which constitute
32 identity theft would, when considered separately, constitute identity
33 theft in the second degree because of value, and the series of
34 transactions are a part of a common scheme or plan, then the
35 transactions may be aggregated in one count and the sum of the value of
36 all of the transactions shall be the value considered in determining
37 the degree of identity theft involved.

1 (6) Every person who, in the commission of identity theft, shall
2 commit any other crime may be punished therefor as well as for the
3 identity theft, and may be prosecuted for each crime separately.

4 (7) A person who violates this section is liable for civil damages
5 of one thousand dollars or actual damages, whichever is greater,
6 including costs to repair the victim's credit record, and reasonable
7 attorneys' fees as determined by the court.

8 ~~((+5))~~ (8) In a proceeding under this section, the crime will be
9 considered to have been committed in any locality where the person
10 whose means of identification or financial information was appropriated
11 resides, or in which any part of the offense took place, regardless of
12 whether the defendant was ever actually in that locality.

13 ~~((+6))~~ (9) The provisions of this section do not apply to any
14 person who obtains another person's driver's license or other form of
15 identification for the sole purpose of misrepresenting his or her age.

16 ~~((+7))~~ (10) In a proceeding under this section in which a person's
17 means of identification or financial information was used without that
18 person's authorization, and when there has been a conviction, the
19 sentencing court may issue such orders as are necessary to correct a
20 public record that contains false information resulting from a
21 violation of this section.

22 **Sec. 4.** RCW 46.20.0921 and 2003 c 214 s 1 are each amended to read
23 as follows:

24 (1) It is a misdemeanor for any person:

25 (a) To display or cause or permit to be displayed or have in his or
26 her possession any fictitious or fraudulently altered driver's license
27 or identicard;

28 (b) To lend his or her driver's license or identicard to any other
29 person or knowingly permit the use thereof by another;

30 (c) To display or represent as one's own any driver's license or
31 identicard not issued to him or her;

32 (d) Willfully to fail or refuse to surrender to the department upon
33 its lawful demand any driver's license or identicard which has been
34 suspended, revoked or canceled;

35 (e) To use a false or fictitious name in any application for a
36 driver's license or identicard or to knowingly make a false statement

1 or to knowingly conceal a material fact or otherwise commit a fraud in
2 any such application;

3 (f) To permit any unlawful use of a driver's license or identicard
4 issued to him or her.

5 (2) It is a class C felony for any person to sell or deliver a
6 stolen driver's license or identicard.

7 (3) It is unlawful for any person to manufacture, sell, or deliver
8 a forged, fictitious, counterfeit, fraudulently altered, or unlawfully
9 issued driver's license or identicard, or to manufacture, sell, or
10 deliver a blank driver's license or identicard except under the
11 direction of the department. A violation of this subsection is:

12 (a) A class C felony if committed (i) for financial gain or (ii)
13 with intent to commit forgery((~~7~~)) or theft((~~7~~ or identity theft)); or

14 (b) A gross misdemeanor if the conduct does not violate (a) of this
15 subsection.

16 (4) Notwithstanding subsection (3) of this section, it is a
17 misdemeanor for any person under the age of twenty-one to manufacture
18 or deliver fewer than four forged, fictitious, counterfeit, or
19 fraudulently altered driver's licenses or identicards for the sole
20 purpose of misrepresenting a person's age.

21 (5) In a proceeding under subsection (1), (2), (3), or (4) of this
22 section that is related to an identity theft under RCW 9.35.020, the
23 crime will be considered to have been committed in any locality where
24 the person whose means of identification or financial information was
25 appropriated resides, or in which any part of the offense took place,
26 regardless of whether the defendant was ever actually in that locality.

--- END ---

BILL REQUEST - CODE REVISER'S OFFICE

BILL REQ. #: S-0127.1/07

ATTY/TYPIST: AI:bat

BRIEF DESCRIPTION: Concerning the filing of police incident reports
for victims of identity theft.

1 AN ACT Relating to identity theft; adding a new section to chapter
2 9.35 RCW; and creating a new section.

3 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

4 NEW SECTION. **Sec. 1.** The legislature finds that victims of
5 identity theft who try to file police incident reports in either the
6 jurisdiction where any part of the crime occurred, or in the
7 jurisdiction in which the victim resides, are sometimes prohibited by
8 the police department from doing so. Several statutes previously
9 passed by the legislature require a victim of identity theft to possess
10 and display a police incident report as a condition of enforcing the
11 rights provided by certain statutes. A police incident report is
12 necessary for an identity theft victim to exercise certain state and
13 federal rights, and is helpful in asserting the rights of others.

14 NEW SECTION. **Sec. 2.** A new section is added to chapter 9.35 RCW
15 to read as follows:

16 (1) A person who has learned or reasonably suspects that his or her
17 financial information or means of identification has been unlawfully
18 obtained, used by, or disclosed to another, as described in this

1 chapter, may file an incident report with a law enforcement agency, by
2 contacting the local law enforcement agency that has jurisdiction over
3 his or her actual residence, place of business, or of the crime. The
4 law enforcement agency shall take a police incident report of the
5 matter and provide the complainant with a copy of that report, and may
6 refer the incident report to another law enforcement agency.

7 (2) Nothing in this section shall be construed to require a law
8 enforcement agency to investigate reports claiming identity theft. An
9 incident report filed under this section is not required to be counted
10 as an open case for purposes of compiling open case statistics.

--- END ---