
HOUSE BILL 3067

State of Washington

59th Legislature

2006 Regular Session

By Representatives Roach, Kirby, Newhouse, Ericks, Sells, P. Sullivan, Green, Rodne, Woods, Strow, Morrell and B. Sullivan

Read first time 01/18/2006. Referred to Committee on Financial Institutions & Insurance.

1 AN ACT Relating to identity theft; amending RCW 19.182.170 and
2 28A.300.460; adding a new section to chapter 43.10 RCW; adding a new
3 chapter to Title 30 RCW; and making appropriations.

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

5 NEW SECTION. **Sec. 1.** The legislature finds that financial fraud
6 and crimes against financial institutions and merchants are increasing
7 exponentially in Washington state. Until recently, these crimes cost
8 businesses and consumers thousands of dollars in losses. They now cost
9 millions of dollars. The legislature further finds that noncredit
10 losses to financial institutions, and credit card, debit card, and
11 check fraud against merchants impose danger to consumers and their
12 financial privacy, and burden law enforcement and public prosecutors
13 with crimes that are difficult to detect and prosecute. The growth in
14 financial fraud also provides opportunities for organized crime and
15 terrorist organizations, and undermines the stability and reliability
16 of financial and other businesses upon which commerce and the economy
17 rely.

18 The legislature intends to enable financial institutions and
19 merchants, to the extent permitted by federal law, to exchange

1 information to prevent, detect, deter, and assist in the prosecution of
2 financial fraud, bank robbery, money laundering, identity theft, and
3 other financial crimes.

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

6 (1) "Designated employees" means security personnel of a financial
7 institution or merchant designated by it to participate in a fraud
8 alert network.

9 (2) "Electronic posting" means the use of a web site or other form
10 of electronic communication used to display information gathered in
11 connection with a fraud alert network.

12 (3) "Financial crimes" means any act, including any anticipatory or
13 completed offense, committed for financial gain, that is chargeable or
14 indictable, regardless of whether the act is actually charged or
15 indicted, as a violation of a state or federal criminal law prohibiting
16 false representation, frauds and swindles in violation of chapter 9.45
17 RCW, forgery, obtaining a signature by deception or duress, criminal
18 impersonation, false certification, unlawful issuance of checks,
19 drafts, funds transfers and payment instructions, identity theft,
20 improperly obtaining financial information, robbery, bank robbery,
21 theft, scams, tax evasion, embezzlement, money laundering, use of
22 proceeds of criminal profiteering, false representation concerning
23 credit, false statement by deposit account applicant, false
24 representation concerning title, forgery of a digital signature or
25 other violation of RCW 9.38.060, burglary when it involves entering the
26 premises of a financial institution or retail establishment, unlawful
27 possession of payment instruments, unlawful production of payment
28 instruments, unlawful possession of a personal identification device,
29 unlawful possession of fictitious identification, unlawful possession
30 of instruments of financial fraud, possession of another's
31 identification, display or possession of a fraudulently issued driver's
32 license or identicard, display or representation as one's own the
33 driver's license or identicard of another person, unlawful factoring of
34 a credit card or payment card transaction, or other state or federal
35 law prohibiting a financial-related crime.

36 (4) "Financial institution" means: (a) Any person doing business
37 under the laws of any state or the United States relating to commercial

1 banks, bank holding companies, financial holding companies, savings
2 banks, savings and loan associations, trust companies, or credit
3 unions; (b) any office of an international banking corporation, branch
4 of a foreign bank, or corporation organized pursuant to the Bank
5 Service Corporation Act (12 U.S.C. Sec. 1861-1867) or a corporation
6 organized under the Edge Act (12 U.S.C. Sec. 611-633); (c)
7 subsidiaries, affiliates, service corporations of the persons in (a)
8 and (b) of this subsection; (d) third-party service providers that
9 provide servicing, processing, account maintenance, or security for the
10 persons in (a), (b), and (c) of this subsection; or (e) any group,
11 organization, or association consisting primarily of the persons in (a)
12 through (c) of this subsection including, without limitation, the
13 Washington bankers association, the American bankers association, and
14 other associations of banks, savings institutions, and/or credit
15 unions, whether inside or outside the state of Washington. However, a
16 group or association in this subsection (4)(e) that obtains access to
17 a fraud alert network may provide access to that network or to
18 information received from that network only to persons described in (a)
19 through (d) of this subsection.

20 (5) "Fraud alert network" means a program established by and among
21 financial institutions and/or merchants to prevent, detect, deter, and
22 assist in the prosecution of financial crimes, including a program in
23 which information is shared by means of electronic posting.

24 (6) "Merchant" means a person engaged in the business of selling,
25 leasing, or distributing goods or services and has an existing
26 contractual relationship or contract with a financial institution and:
27 (a) Has a physical presence in the state that consumers may patronize
28 to make purchases of goods or services; (b) is physically located in
29 the state and sells goods or services to residents of the state via the
30 internet; or (c) is an association or cooperative organization of
31 persons in (a) and (b) of this subsection.

32 (7) "Participant" means a financial institution or merchant that
33 participates in a fraud alert network.

34 NEW SECTION. **Sec. 3.** (1) This chapter provides immunity from
35 liability for financial institutions and merchants who participate in
36 a fraud alert network and who comply with the provisions of this

1 chapter and the standards of use set forth in this subsection as
2 follows:

3 (a) Access to the fraud alert network is private and limited to
4 financial institutions, merchants, and law enforcement agencies;

5 (b) The sole purpose of the fraud alert network is to share
6 information among financial institutions, merchants, and law
7 enforcement agencies to prevent, detect, deter, and assist in the
8 prosecution of financial crimes;

9 (c) Information furnished to the fraud alert network consists of:

10 (i) Descriptions of recent actual or suspected financial crimes
11 perpetrated against or coming to the attention of the participant
12 furnishing the information; (ii) descriptions, photographs, images,
13 reproductions, fingerprints, identifying features, traits, habits,
14 background, or other data related to identifying the person, persons,
15 or groups suspected of committing, aiding, or abetting financial
16 crimes; (iii) identifying information regarding methods of operation,
17 devices, tricks, or schemes used by persons suspected of financial
18 crimes; (iv) descriptions, photographs, images, or reproductions of
19 writings, communications, checks, and personal identification used in
20 connection with suspected financial crimes; (v) descriptions,
21 photographs, images, or reproductions of vehicles, license plates,
22 weapons, devices, or other things used in connection with suspected
23 financial crimes; (vi) cautionary statements regarding suspects, for
24 example a statement that a suspect is armed and dangerous; and (vii)
25 other information that allows participants to identify financial
26 crimes, to identify persons suspected in connection with financial
27 crimes, to assist in the apprehension of persons suspected of financial
28 crimes, or to contact others for further information;

29 (d) Information furnished to the fraud alert network may not
30 consist of delinquent payment information, nor may it consist of other
31 similar evidence of a person's credit history, except in the
32 exceptional instance where such evidence is an integral part of
33 information provided under (c) of this subsection and is reasonably
34 believed to be related to a financial crime;

35 (e) Information posted must be accessible only to designated
36 employees, and the distribution of information is limited to those
37 employees, attorneys, and agents of participants who have job-related

1 duties relevant to the use of such information in connection with
2 preventing, detecting, deterring, or assisting in the prosecution of
3 financial crimes;

4 (f) The fraud alert network has procedures reasonably calculated to
5 ensure the security of the information obtained;

6 (g) Users of the fraud alert network are informed that the
7 information obtained from the fraud alert network may not be used to
8 evaluate and make decisions about applications for loans, lines of
9 credit, and credit cards;

10 (h) Information furnished pursuant to the fraud alert network is
11 limited to statements of fact that the person furnishing the
12 information reasonably believes to be true. However, in exigent
13 circumstances, information may be furnished without such reasonable
14 belief if the circumstances creating an emergency are described, and
15 cautionary advice is provided regarding the limited knowledge of the
16 person furnishing the information; and

17 (i) The fraud alert network has an operator that: (i) Employs
18 procedures to promptly correct and erase information that the operator
19 learns is erroneous or was submitted or posted to the fraud alert
20 network not in compliance with this section; (ii) takes reasonable
21 steps to limit access to the fraud alert network to financial
22 institutions, merchants, and law enforcement agencies; and (iii) denies
23 access to the fraud alert network to persons who are not financial
24 institutions, merchants, or law enforcement agencies or who do not
25 abide by the provisions of this chapter.

26 (2) Washington law governs the operation of a fraud alert network.
27 A participant or law enforcement agency that participates in a fraud
28 alert network in accordance with subsection (1) of this section,
29 whether through furnishing, posting, communicating, or using
30 information in connection thereto, has immunity from civil liability
31 under the laws of the state of Washington and its political
32 subdivisions and, to the extent the conflicts of law rules of any other
33 jurisdiction refer to the law of the state of Washington, under the
34 laws and rules of such other jurisdiction and its political
35 subdivisions. However, this immunity does not apply to statutory
36 violations.

37 (3) Any financial institution or merchant that makes a voluntary
38 disclosure of any possible violation of law or regulation to a federal,

1 state, or local government or agency in connection with information
2 obtained from a fraud alert network is immune from civil liability for
3 such disclosure or for any failure to provide notice of such disclosure
4 to the person who is the subject of or identified in the disclosure,
5 under the laws and rules of the state of Washington and its political
6 subdivisions and, to the extent the conflicts of law rules of any other
7 jurisdiction refer to the law of the state of Washington, under the
8 laws and rules of such other jurisdiction and its political
9 subdivisions, and under any contract or other legally enforceable
10 agreement.

11 NEW SECTION. **Sec. 4.** The immunity under section 3 of this act
12 does not apply to any participant that:

13 (1) Provides false information to the fraud alert network that the
14 participant does not reasonably believe to be true. However, in
15 exigent circumstances, information may be furnished without that
16 reasonable belief if the circumstances creating an emergency are
17 described, and cautionary advice is provided regarding the limited
18 knowledge of the person furnishing the information;

19 (2) Fails to maintain review procedures to remove or correct false,
20 outdated, incomplete, or erroneous information furnished by it to the
21 fraud alert network;

22 (3) Fails to maintain procedures to ensure that information
23 obtained from the fraud alert network is provided only to employees,
24 attorneys, or agents who have job-related duties relevant to the use of
25 such information;

26 (4) Uses information obtained from the fraud alert network to
27 evaluate and make decisions about applications for loans, lines of
28 credit, and credit cards;

29 (5) Uses information for a purpose other than preventing,
30 detecting, deterring, and assisting in the prosecution of financial
31 crimes;

32 (6) Uses, reproduces, distributes, publishes, forwards, shares,
33 sells, or communicates any information obtained from the fraud alert
34 network for a commercial purpose, such as for advertising or marketing;
35 or

36 (7) Provides, sells, or resells access to the fraud alert network
37 to a person who is not a participant.

1 NEW SECTION. **Sec. 5.** (1) It is the intent of this chapter to
2 encourage the sharing of information consistent with federal law.

3 (2) It is intended that so long as the participants comply with
4 this chapter, the provisions of the Washington fair credit reporting
5 act, chapter 19.182 RCW, do not apply to the fraud alert network.
6 However, if it is determined that the federal fair credit reporting act
7 applies to a fraud alert network, the Washington fair credit reporting
8 act also applies.

9 NEW SECTION. **Sec. 6.** (1) The fraud alert network and its
10 participants shall notify the public regarding the existence of the
11 fraud alert network and how it functions. This notice must include a
12 description of the purpose of the network, how the network shares
13 information, the types of information furnished to the network, how
14 consumer complaints may be registered, and the procedures available to
15 an individual for the correction or removal of incomplete, inaccurate,
16 or erroneous information.

17 (2) The public notice required of the fraud alert network and its
18 participants under subsection (1) of this section must, at a minimum,
19 include:

20 (a) A toll-free telephone number maintained by the network that may
21 be called by individuals in order to obtain the information required
22 under subsection (1) of this section;

23 (b) An internet web site maintained by the network that provides
24 the public with the information required under subsection (1) of this
25 section;

26 (c) Written pamphlets that are made conspicuously available at each
27 place of business of a network participant, and that contain the
28 information required under subsection (1) of this section as well as
29 the toll-free telephone number and web site address maintained by the
30 network; and

31 (d) A conspicuously posted sign at each place of business of a
32 network participant that notifies the public of the business's
33 participation in the fraud alert network and that includes both the
34 toll-free telephone number and web site address required under this
35 section.

36 (3) The fraud alert network may not begin operating until the
37 public notice provisions required under this section are implemented.

1 NEW SECTION. **Sec. 7.** (1) By January 1, 2007, and again by January
2 1, 2008, the organizing body representing participants in the fraud
3 alert network shall provide a comprehensive written report to the house
4 financial institutions and insurance committee and the senate committee
5 on financial institutions, housing, and consumer protection regarding
6 the implementation of this chapter.

7 (2) The written report must include the following:

8 (a) The number of participants in the network, including the name
9 of each participating entity;

10 (b) The standards or protocols established by the network to
11 determine compliance on the part of a participant with this chapter;

12 (c) A detailed description of the procedures that are adopted by
13 the fraud alert network, as required under section 3 of this act, to
14 ensure the security and accuracy of information furnished to the
15 network, including procedures for the removal or correction of
16 incomplete or erroneous information furnished to the network;

17 (d) A detailed description of the procedures adopted by the network
18 by which an individual who has been reported to the network, or who is
19 the subject of any information furnished to the network, may correct or
20 remove inaccurate, incomplete, or erroneous information;

21 (e) An accounting of how many actions the network has taken in the
22 preceding year to correct or remove incomplete or erroneous information
23 from the network, including how many actions were the result of a
24 request or complaint from an individual whose information has been
25 entered into the network;

26 (f) The number of complaints about the fraud alert network received
27 by each participant in the network, including a description of each
28 complaint and what actions, either on the part of the network
29 participant or the complainant, resulted from each complaint;

30 (g) A description of any adverse action taken by the fraud alert
31 network against a network participant resulting from noncompliance with
32 the standards and procedures established by the network as a condition
33 of participation in the network; and

34 (h) The disclosure of the number of individuals whose names have
35 been placed in the network data base for suspected financial crimes and
36 a description of the type of alleged illegal activity that led to the
37 individuals being placed in the network data base.

1 NEW SECTION. **Sec. 8.** This chapter shall be construed to encourage
2 the sharing of information by financial institutions, merchants, and
3 law enforcement for the prevention and prosecution of financial fraud.

4 NEW SECTION. **Sec. 9.** This chapter may be known and cited as the
5 financial fraud alert act.

6 NEW SECTION. **Sec. 10.** If any part of sections 1 through 9 of this
7 act is found to be in conflict with federal requirements that are a
8 prescribed condition to the allocation of federal funds to the state,
9 the conflicting part of this act is inoperative solely to the extent of
10 the conflict and with respect to the agencies directly affected, and
11 this finding does not affect the operation of the remainder of this act
12 in its application to the agencies concerned.

13 NEW SECTION. **Sec. 11.** Sections 1 through 10 of this act
14 constitute a new chapter in Title 30 RCW.

15 **Sec. 12.** RCW 19.182.170 and 2005 c 342 s 1 are each amended to
16 read as follows:

17 (1) (~~(A victim of identity theft who has submitted a valid police~~
18 ~~report to a consumer reporting agency)) Except under this section, a
19 consumer may elect to place a security freeze on his or her report by
20 making a request in writing by certified mail to a consumer reporting
21 agency. "Security freeze" means a notice placed in a consumer's credit
22 report, at the request of the consumer and subject to certain
23 exceptions, that prohibits the consumer reporting agency from releasing
24 the consumer's credit report or any information from it without the
25 express authorization of the consumer. If a security freeze is in
26 place, information from a consumer's credit report may not be released
27 to a third party without prior express authorization from the consumer.
28 This subsection does not prevent a consumer reporting agency from
29 advising a third party that a security freeze is in effect with respect
30 to the consumer's credit report.~~

31 (2) For purposes of this section and RCW 19.182.180 through
32 19.182.210, a "victim of identity theft" means:

33 (a) A victim of identity theft as defined in RCW 9.35.020; or

1 (b) A person who has been notified by an agency, person, or
2 business that owns or licenses computerized data of a breach in a
3 computerized data system which has resulted in the acquisition of that
4 person's unencrypted personal information by an unauthorized person or
5 entity.

6 (3) A consumer reporting agency shall place a security freeze on a
7 consumer's credit report no later than five business days
8 after receiving a written request from the consumer.

9 (4) The consumer reporting agency shall send a written confirmation
10 of the security freeze to the consumer within ten business days and
11 shall provide the consumer with a unique personal identification number
12 or password to be used by the consumer when providing authorization for
13 the release of his or her credit report for a specific party or period
14 of time.

15 (5) If the consumer wishes to allow his or her credit report to be
16 accessed for a specific party or period of time while a freeze is in
17 place, he or she shall contact the consumer reporting agency, request
18 that the freeze be temporarily lifted, and provide the following:

19 (a) Proper identification, which means that information generally
20 deemed sufficient to identify a person. Only if the consumer is unable
21 to sufficiently identify himself or herself, may a consumer reporting
22 agency require additional information concerning the consumer's
23 employment and personal or family history in order to verify his or her
24 identity;

25 (b) The unique personal identification number or password provided
26 by the credit reporting agency under subsection (4) of this section;
27 and

28 (c) The proper information regarding the third party who is to
29 receive the credit report or the time period for which the report is
30 available to users of the credit report.

31 (6) A consumer reporting agency that receives a request from a
32 consumer to temporarily lift a freeze on a credit report under
33 subsection (5) of this section((7)) shall comply with the request no
34 later than three business days after receiving the request.

35 (7) A consumer reporting agency may develop procedures involving
36 the use of telephone, fax, the internet, or other electronic media to
37 receive and process a request from a consumer to temporarily lift a

1 freeze on a credit report under subsection (5) of this section in an
2 expedited manner.

3 (8) A consumer reporting agency shall remove or temporarily lift a
4 freeze placed on a consumer's credit report only in the following
5 cases:

6 (a) Upon consumer request, under subsection (5) or (11) of this
7 section; or

8 (b) When the consumer's credit report was frozen due to a material
9 misrepresentation of fact by the consumer. When a consumer reporting
10 agency intends to remove a freeze upon a consumer's credit report under
11 this subsection, the consumer reporting agency shall notify the
12 consumer in writing prior to removing the freeze on the consumer's
13 credit report.

14 (9) When a third party requests access to a consumer credit report
15 on which a security freeze is in effect, and this request is in
16 connection with an application for credit or any other use, and the
17 consumer does not allow his or her credit report to be accessed for
18 that specific party or period of time, the third party may treat the
19 application as incomplete.

20 (10) When a consumer requests a security freeze, the consumer
21 reporting agency shall disclose the process of placing and temporarily
22 lifting a freeze, and the process for allowing access to information
23 from the consumer's credit report for a specific party or period of
24 time while the freeze is in place.

25 (11) A security freeze remains in place until the consumer requests
26 that the security freeze be removed or the security freeze expires.

27 (a) A consumer reporting agency shall remove a security freeze
28 within three business days of receiving a request for removal from the
29 consumer, who provides both of the following:

30 ~~((a))~~ (i) Proper identification, as defined in subsection (5)(a)
31 of this section; and

32 ~~((b))~~ (ii) The unique personal identification number or password
33 provided by the consumer reporting agency under subsection (4) of this
34 section.

35 (b) A security freeze expires two years after the date it is put in
36 place by the consumer reporting agency unless the consumer is a member
37 of the national guard on active duty or the United States military on
38 active duty.

1 (12)(a) A consumer reporting agency may not charge a victim of
2 identity theft a fee to place or remove a security freeze.

3 (b) A consumer reporting agency may charge a reasonable fee, not to
4 exceed ten dollars, to consumers that are not victims of identity theft
5 and are sixty-five years or older.

6 (c) A consumer reporting agency may charge a reasonable fee, not to
7 exceed twenty-five dollars, to consumers that are not victims of
8 identity theft and are less than sixty-five years of age.

9 (13) This section does not apply to the use of a consumer credit
10 report by any of the following:

11 (a) A person or entity, or a subsidiary, affiliate, or agent of
12 that person or entity, or an assignee of a financial obligation owing
13 by the consumer to that person or entity, or a prospective assignee of
14 a financial obligation owing by the consumer to that person or entity
15 in conjunction with the proposed purchase of the financial obligation,
16 with which the consumer has or had prior to assignment an account or
17 contract, including a demand deposit account, or to whom the consumer
18 issued a negotiable instrument, for the purposes of reviewing the
19 account or collecting the financial obligation owing for the account,
20 contract, or negotiable instrument. For purposes of this subsection,
21 "reviewing the account" includes activities related to account
22 maintenance, monitoring, credit line increases, and account upgrades
23 and enhancements;

24 (b) A subsidiary, affiliate, agent, assignee, or prospective
25 assignee of a person to whom access has been granted under subsection
26 (5) of this section for purposes of facilitating the extension of
27 credit or other permissible use;

28 (c) Any federal, state, or local entity, including a law
29 enforcement agency, court, or their agents or assigns;

30 (d) A private collection agency acting under a court order,
31 warrant, or subpoena;

32 (e) A child support agency acting under Title IV-D of the social
33 security act (42 U.S.C. et seq.);

34 (f) The department of social and health services acting to fulfill
35 any of its statutory responsibilities;

36 (g) The internal revenue service acting to investigate or collect
37 delinquent taxes or unpaid court orders or to fulfill any of its other
38 statutory responsibilities;

1 (h) The use of credit information for the purposes of prescreening
2 as provided for by the federal fair credit reporting act;

3 (i) Any person or entity administering a credit file monitoring
4 subscription service to which the consumer has subscribed; ~~((and))~~

5 (j) Any person or entity for the purpose of providing a consumer
6 with a copy of his or her credit report upon the consumer's request;

7 (k) An insurance company authorized to do business in Washington
8 state;

9 (l) A mortgage broker licensed and regulated by the department of
10 financial institutions; and

11 (m) A vehicle dealer as defined in RCW 46.70.011.

12 (14) A consumer reporting agency is not required to place more than
13 ten thousand security freezes at any one time. If a consumer reporting
14 agency does not place a security freeze because the ten thousand
15 maximum is met, the consumer reporting agency must place the consumer
16 on a list based on when the request for a security freeze was received
17 by the consumer reporting agency. The first name on the list is the
18 consumer whose request was received first. When a security freeze is
19 removed or expires, the consumer reporting agency must place a freeze
20 on the credit report of the consumer who is first on the list. A
21 consumer who is a member of the national guard on active duty or the
22 United States military on active duty does not count toward the total
23 number of security freezes.

24 (15) For the purpose of this section, "active duty" means deployed
25 outside the United States.

26 **Sec. 13.** RCW 28A.300.460 and 2004 c 247 s 5 are each amended to
27 read as follows:

28 The task of the financial literacy public-private partnership is to
29 seek out and determine the best methods of equipping students with the
30 knowledge and skills they need, before they become self-supporting, in
31 order for them to make critical decisions regarding their personal
32 finances. The components of personal financial literacy examined shall
33 include, at a minimum, consumer financial education, personal finance,
34 strategies to safeguard personal information and to recover from
35 identity theft, and personal credit. The partnership shall identify
36 the types of outcome measures expected from participating students, in

1 accordance with the definitions and outcomes developed under RCW
2 28A.300.455.

3 NEW SECTION. **Sec. 14.** (1) The sum of twenty-five thousand
4 dollars, or as much thereof as may be necessary, is appropriated for
5 the fiscal year ending June 30, 2007, from the general fund to the
6 Washington financial literacy public-private partnership account for
7 the purposes of RCW 28A.300.465.

8 (2) The sum of twenty-five thousand dollars, or as much thereof as
9 may be necessary, is appropriated for the fiscal year ending June 30,
10 2008, from the general fund to the Washington financial literacy
11 public-private partnership account for the purposes of RCW 28A.300.465.

12 (3) The amounts in this section are provided solely for the
13 purposes of RCW 28A.300.465. The superintendent of public instruction
14 or the superintendent's designee may authorize expenditure of the
15 amounts provided in this section when equal matching amounts from
16 nonstate sources are received in the Washington financial literacy
17 public-private partnership account.

18 NEW SECTION. **Sec. 15.** A new section is added to chapter 43.10 RCW
19 to read as follows:

20 (1) The attorney general shall develop a grant program to provide
21 funding for persons and organizations that provide:

- 22 (a) Education to aid seniors in preventing identity theft;
23 (b) Assistance to aid seniors in recovering from identity theft;
24 (c) Education to aid persons with a developmental disability and
25 their legal representatives in preventing the theft of the identity of
26 persons with a developmental disability;
27 (d) Assistance to aid persons with a developmental disability and
28 their legal representatives in recovering from the identity theft of
29 the identity of persons with a developmental disability; or
30 (e) Any combination of the above.

31 (2) The attorney general shall make an annual report regarding the
32 development and the implementation of the grant program to the
33 legislature by December 1st. The first report is due December 1, 2007.

34 NEW SECTION. **Sec. 16.** The sum of one million five hundred
35 thousand dollars, or as much thereof as may be necessary, is

1 appropriated for the fiscal year ending June 30, 2007, from the general
2 fund to the attorney general for the purposes of section 15 of this
3 act.

--- END ---