

1 A bill to be entitled
2 An act relating to consumer protection;
3 creating s. 817.5681, F.S.; requiring business
4 persons maintaining computerized data that
5 includes personal information to provide notice
6 of breaches of system security under certain
7 circumstances; providing requirements;
8 providing for administrative fines; providing
9 exceptions and limitations; authorizing delays
10 of such disclosures under certain
11 circumstances; providing definitions; providing
12 for alternative notice methods; specifying
13 conditions of compliance for persons
14 maintaining certain alternative notification
15 procedures; specifying conditions under which
16 notification is not required; providing
17 requirements for documentation and maintenance
18 of documentation; providing an administrative
19 fine for failing to document certain failures
20 to comply; providing for application of
21 administrative sanctions to certain persons
22 under certain circumstances; authorizing the
23 Department of Legal Affairs to institute
24 proceedings to assess and collect fines;
25 requiring notification of consumer reporting
26 agencies of breaches of system security under
27 certain circumstances; amending s. 817.568,
28 F.S.; redefining the term "personal
29 identification information" and defining the
30 term "counterfeit or fictitious personal
31 identification information"; revising criminal

1 penalties relating to the offense of
 2 fraudulently using, or possessing with intent
 3 to fraudulently use, personal identification
 4 information; providing minimum mandatory terms
 5 of imprisonment; creating the offenses of
 6 willfully and fraudulently using, or possessing
 7 with intent to fraudulently use, personal
 8 identification information concerning a
 9 deceased individual; providing criminal
 10 penalties; providing for minimum mandatory
 11 terms of imprisonment; creating the offense of
 12 willfully and fraudulently creating or using,
 13 or possessing with intent to fraudulently use,
 14 counterfeit or fictitious personal
 15 identification information; providing criminal
 16 penalties; providing for reclassification of
 17 offenses under certain circumstances; providing
 18 for reduction or suspension of sentences under
 19 certain circumstances; providing for
 20 severability; providing an effective date.

21
 22 Be It Enacted by the Legislature of the State of Florida:

23
 24 Section 1. Section 817.5681, Florida Statutes, is
 25 created to read:

26 817.5681 Breach of security concerning confidential
 27 personal information in third-party possession; administrative
 28 penalties.--

29 (1)(a) Any person who conducts business in this state
 30 and maintains computerized data in a system that includes
 31 personal information shall provide notice of any breach of the

1 security of the system, following a determination of the
2 breach, to any resident of this state whose unencrypted
3 personal information was, or is reasonably believed to have
4 been, acquired by an unauthorized person. The notification
5 shall be made without unreasonable delay, consistent with the
6 legitimate needs of law enforcement, as provided in subsection
7 (3) and paragraph (10)(a), or subject to any measures
8 necessary to determine the presence, nature, and scope of the
9 breach and restore the reasonable integrity of the system.
10 Notification must be made no later than 45 days following the
11 determination of the breach unless otherwise provided in this
12 section.

13 (b) Any person required to make notification under
14 paragraph (a) who fails to do so within 45 days following the
15 determination of a breach or receipt of notice from law
16 enforcement as provided in subsection (3) is liable for an
17 administrative fine not to exceed \$500,000, as follows:

18 1. In the amount of \$1,000 for each day the breach
19 goes undisclosed for up to 30 days and, thereafter, \$50,000
20 for each 30-day period or portion thereof for up to 180 days.

21 2. If notification is not made within 180 days, any
22 person required to make notification under paragraph (a) who
23 fails to do so is subject to an administrative fine of up to
24 \$500,000.

25 (c) The administrative sanctions for failure to notify
26 in paragraph (b) apply per breach, and not per individual
27 affected by the breach. Such sanctions do not apply in the
28 case of personal information in the custody of any
29 governmental agency or subdivision, unless that governmental
30 agency or subdivision has entered into a contract with a
31 contractor or third-party administrator to provide

1 governmental services. In such case, the contractor or
2 third-party administrator is the person to whom such sanctions
3 apply and such contractor or third-party administrator found
4 in violation of such notification requirements has no right to
5 any contribution or set-off that may otherwise be available
6 against the employing agency or subdivision.

7 (2)(a) Any person who maintains computerized data that
8 includes personal information on behalf of another business
9 entity shall disclose to the business entity for which the
10 information is maintained any breach of the security of the
11 system as soon as practicable, but no later than 10 days
12 following the determination, if the personal information was,
13 or is reasonably believed to have been, acquired by an
14 unauthorized person. The person who maintains the data on
15 behalf of another business entity and the business entity on
16 whose behalf the data is maintained may agree who will provide
17 the notice, if any is required, as provided in paragraph
18 (1)(a); however, only a single notice for each breach of the
19 security of the system is required. If agreement regarding
20 notification cannot be reached, the person who has the direct
21 business relationship with the resident of this state must
22 provide the notice required under paragraph (1)(a).

23 (b) Any person required to disclose to a business
24 entity under paragraph (a) who fails to do so within 10 days
25 after the determination of a breach or receipt of notification
26 from law enforcement as provided in subsection (3) is liable
27 for an administrative fine not to exceed \$500,000, as follows:

28 1. In the amount of \$1,000 for each day the breach
29 goes undisclosed for up to 30 days and, thereafter, \$50,000
30 for each 30-day period or portion thereof for up to 180 days.

31

1 2. If disclosure is not made within 180 days, such
2 person is subject to an administrative fine of up to \$500,000.

3 (c) The administrative sanctions for nondisclosure
4 provided in paragraph (b) apply per breach, and not per
5 individual affected by the breach. Such sanctions do not
6 apply in the case of personal information in the custody of
7 any governmental agency or subdivision unless that
8 governmental agency or subdivision has entered into a contract
9 with a contractor or third-party administrator to provide
10 governmental services. In such case, the contractor or
11 third-party administrator is the person to whom such sanctions
12 apply and such contractor or third-party administrator found
13 in violation of such nondisclosure restrictions has no right
14 to any contribution or set-off that may otherwise be available
15 against the employing agency or subdivision.

16 (3) The notification required by this section may be
17 delayed upon a request by law enforcement if a law enforcement
18 agency determines that the notification will impede a criminal
19 investigation. The notification time period required by this
20 section shall commence after the person receives notice from
21 the law enforcement agency that the notification will not
22 compromise the investigation.

23 (4) For purposes of this section, the terms "breach"
24 and "breach of the security of the system" mean unlawful and
25 unauthorized acquisition of computerized data that materially
26 compromises the security, confidentiality, or integrity of
27 personal information maintained by the person. Good faith
28 acquisition of personal information by an employee or agent of
29 the person is not a breach or breach of the security of the
30 system, provided the information is not used for a purpose
31

1 unrelated to the business or subject to further unauthorized
2 use.

3 (5) For purposes of this section, the term "personal
4 information" means an individual's first name, first initial
5 and last name, or any middle name and last name, in
6 combination with any one or more of the following data
7 elements when the data elements are not encrypted:

8 (a) Social security number.

9 (b) Driver's license number or Florida Identification
10 Card number.

11 (c) Account number, credit card number, or debit card
12 number, in combination with any required security code, access
13 code, or password that would permit access to an individual's
14 financial account.

15
16 The term does not include publicly available information that
17 is lawfully made available to the general public from federal,
18 state, or local government records or widely distributed
19 media.

20 (6) For purposes of this section, notice may be
21 provided by one of the following methods:

22 (a) Written notice;

23 (b) Electronic notice, if the notice provided is
24 consistent with the provisions regarding electronic records
25 and signatures in 15 U.S.C. s. 7001 or if the person or
26 business providing the notice has a valid e-mail address for
27 the subject person and the subject person has agreed to accept
28 communications electronically; or

29 (c) Substitute notice, if the person demonstrates that
30 the cost of providing notice would exceed \$250,000, the
31 affected class of subject persons to be notified exceeds

1 500,000, or the person does not have sufficient contact
2 information. Substitute notice shall consist of all of the
3 following:

4 1. Electronic mail or e-mail notice when the person
5 has an electronic mail or e-mail address for the subject
6 persons.

7 2. Conspicuous posting of the notice on the web page
8 of the person, if the person maintains a web page.

9 3. Notification to major statewide media.

10 (7) For purposes of this section, the term
11 "unauthorized person" means any person who does not have
12 permission from, or a password issued by, the person who
13 stores the computerized data to acquire such data, but does
14 not include any individual to whom the personal information
15 pertains.

16 (8) For purposes of this section, the term "person"
17 means a person as defined in s. 1.01. For purposes of this
18 section, the State of Florida, as well as any of its agencies
19 or political subdivisions, and any of the agencies of its
20 political subdivisions, is a person.

21 (9) Notwithstanding subsection (6), a person who
22 maintains:

23 (a) The person's own notification procedures as part
24 of an information security or privacy policy for the treatment
25 of personal information, which procedures are otherwise
26 consistent with the timing requirements of this part; or

27 (b) A notification procedure pursuant to the rules,
28 regulations, procedures, or guidelines established by the
29 person's primary or functional federal regulator,
30
31

1 shall be deemed to be in compliance with the notification
2 requirements of this section if the person notifies subject
3 persons in accordance with the person's policies or the rules,
4 regulations, procedures, or guidelines established by the
5 primary or functional federal regulator in the event of a
6 breach of security of the system.

7 (10)(a) Notwithstanding subsection (2), disclosure is
8 not required if, after an appropriate investigation or after
9 consultation with relevant federal, state, and local agencies
10 responsible for law enforcement, the person reasonably
11 determines that the breach has not and will not likely result
12 in harm to the individuals whose personal information has been
13 acquired and accessed. Such a determination must be documented
14 in writing and the documentation must be maintained for 5
15 years.

16 (b) Any person required to document a failure to
17 notify affected persons who fails to document the failure as
18 required in paragraph (a) or who, if documentation was
19 created, fails to maintain the documentation as required in
20 paragraph (a) is liable for an administrative fine of up to
21 \$50,000 for such failure.

22 (c) The administrative sanctions in paragraph (b) do
23 not apply in the case of personal information in the custody
24 of any governmental agency or subdivision, unless that
25 governmental agency or subdivision has entered into a contract
26 with a contractor or third-party administrator to provide
27 governmental services. In such case the contractor or
28 third-party administrator is the person to whom such sanctions
29 apply and such contractor or third-party administrator found
30 in violation of the documentation and maintenance of
31 documentation requirements has no right to any contribution or

1 set-off that may otherwise be available against the employing
2 agency or subdivision.

3 (11) The Department of Legal Affairs may institute
4 proceedings to assess and collect the fines authorized in this
5 section.

6 (12) If a person discovers circumstances requiring
7 notification pursuant to this section of more than 1,000
8 persons at a single time, the person shall also notify,
9 without unreasonable delay, all consumer reporting agencies
10 that compile and maintain files on consumers on a nationwide
11 basis, as defined in 15 U.S.C. s. 1681a(p), of the timing,
12 distribution, and content of the notices.

13 Section 2. Section 817.568, Florida Statutes, is
14 amended to read:

15 817.568 Criminal use of personal identification
16 information.--

17 (1) As used in this section, the term:

18 (a) "Access device" means any card, plate, code,
19 account number, electronic serial number, mobile
20 identification number, personal identification number, or
21 other telecommunications service, equipment, or instrument
22 identifier, or other means of account access that can be used,
23 alone or in conjunction with another access device, to obtain
24 money, goods, services, or any other thing of value, or that
25 can be used to initiate a transfer of funds, other than a
26 transfer originated solely by paper instrument.

27 (b) "Authorization" means empowerment, permission, or
28 competence to act.

29 (c) "Harass" means to engage in conduct directed at a
30 specific person that is intended to cause substantial
31 emotional distress to such person and serves no legitimate

1 purpose. "Harass" does not mean to use personal identification
2 information for accepted commercial purposes. The term does
3 not include constitutionally protected conduct such as
4 organized protests or the use of personal identification
5 information for accepted commercial purposes.

6 (d) "Individual" means a single human being and does
7 not mean a firm, association of individuals, corporation,
8 partnership, joint venture, sole proprietorship, or any other
9 entity.

10 (e) "Person" means a "person" as defined in s.
11 1.01(3).

12 (f) "Personal identification information" means any
13 name or number that may be used, alone or in conjunction with
14 any other information, to identify a specific individual,
15 including any:

16 1. Name, postal or electronic mail address, telephone
17 number, social security number, date of birth, mother's maiden
18 name, official state-issued or United States-issued driver's
19 license or identification number, alien registration number,
20 government passport number, employer or taxpayer
21 identification number, Medicaid or food stamp account number,
22 ~~or~~ bank account number, ~~or~~ credit or debit card number, or
23 personal identification number or code assigned to the holder
24 of a debit card by the issuer to permit authorized electronic
25 use of such card;

26 2. Unique biometric data, such as fingerprint, voice
27 print, retina or iris image, or other unique physical
28 representation;

29 3. Unique electronic identification number, address,
30 or routing code; ~~or~~

31 4. Medical records;

1 ~~5.4-~~ Telecommunication identifying information or
2 access device; ~~or-~~

3 6. Other number or information that can be used to
4 access a person's financial resources.

5 (g) "Counterfeit or fictitious personal identification
6 information" means any counterfeit, fictitious, or fabricated
7 information in the similitude of the data outlined in
8 paragraph (f) that, although not truthful or accurate, would
9 in context lead a reasonably prudent person to credit its
10 truthfulness and accuracy.

11 (2)(a) Any person who willfully and without
12 authorization fraudulently uses, or possesses with intent to
13 fraudulently use, personal identification information
14 concerning an individual without first obtaining that
15 individual's consent, commits the offense of fraudulent use of
16 personal identification information, which is a felony of the
17 third degree, punishable as provided in s. 775.082, s.
18 775.083, or s. 775.084.

19 (b) Any person who willfully and without authorization
20 fraudulently uses personal identification information
21 concerning an individual without first obtaining that
22 individual's consent commits a felony of the second degree,
23 punishable as provided in s. 775.082, s. 775.083, or s.
24 775.084, if the pecuniary benefit, the value of the services
25 received, the payment sought to be avoided, or the amount of
26 the injury or fraud perpetrated is \$5,000 or more or if the
27 person fraudulently uses the personal identification
28 information of 10 or more individuals, but fewer than 20
29 individuals, without their consent. Notwithstanding any other
30 provision of law, the court shall sentence any person
31 convicted of committing the offense described in this

1 paragraph to a mandatory minimum sentence of 3 years'
2 imprisonment.

3 (c) Any person who willfully and without authorization
4 fraudulently uses personal identification information
5 concerning an individual without first obtaining that
6 individual's consent commits a felony of the first degree,
7 punishable as provided in s. 775.082, s. 775.083, or s.
8 775.084, if the pecuniary benefit, the value of the services
9 received, the payment sought to be avoided, or the amount of
10 the injury or fraud perpetrated is \$50,000 or more or if the
11 person fraudulently uses the personal identification
12 information of 20 or more individuals, but fewer than 30
13 individuals, without their consent. Notwithstanding any other
14 provision of law, the court shall sentence any person
15 convicted of committing the offense described in this
16 paragraph+

17 ~~1.~~ to a mandatory minimum sentence of 5 years'
18 imprisonment. If the pecuniary benefit, the value of the
19 services received, the payment sought to be avoided, or the
20 amount of the injury or fraud perpetrated is \$100,000 or more,
21 or if the person fraudulently uses the personal identification
22 information of 30 or more individuals without their consent,
23 notwithstanding any other law, the court shall sentence any
24 person convicted of committing the offense described in this
25 paragraph

26 ~~2.~~ to a mandatory minimum sentence of 10 years'
27 imprisonment, ~~if the pecuniary benefit, the value of the~~
28 ~~services received, the payment sought to be avoided, or the~~
29 ~~amount of the injury or fraud perpetrated is \$100,000 or more~~
30 ~~or if the person fraudulently uses the personal identification~~
31 ~~information of 30 or more individuals without their consent.~~

1 (3) Neither paragraph (2)(b) nor paragraph (2)(c)
2 prevents a court from imposing a greater sentence of
3 incarceration as authorized by law. If the minimum mandatory
4 terms of imprisonment imposed under paragraph (2)(b) or
5 paragraph (2)(c) exceed the maximum sentences authorized under
6 s. 775.082, s. 775.084, or the Criminal Punishment Code under
7 chapter 921, the mandatory minimum sentence must be imposed.
8 If the mandatory minimum terms of imprisonment under paragraph
9 (2)(b) or paragraph (2)(c) are less than the sentence that
10 could be imposed under s. 775.082, s. 775.084, or the Criminal
11 Punishment Code under chapter 921, the sentence imposed by the
12 court must include the mandatory minimum term of imprisonment
13 as required by paragraph (2)(b) or paragraph (2)(c).

14 (4) A ~~Any~~ person who willfully and without
15 authorization possesses, uses, or attempts to use personal
16 identification information concerning an individual without
17 first obtaining that individual's consent, and who does so for
18 the purpose of harassing that individual, commits the offense
19 of harassment by use of personal identification information,
20 which is a misdemeanor of the first degree, punishable as
21 provided in s. 775.082 or s. 775.083.

22 (5) If an offense prohibited under this section was
23 facilitated or furthered by the use of a public record, as
24 defined in s. 119.011, the offense is reclassified to the next
25 higher degree as follows:

26 (a) A misdemeanor of the first degree is reclassified
27 as a felony of the third degree.

28 (b) A felony of the third degree is reclassified as a
29 felony of the second degree.

30 (c) A felony of the second degree is reclassified as a
31 felony of the first degree.

1
2 For purposes of sentencing under chapter 921 and incentive
3 gain-time eligibility under chapter 944, a felony offense that
4 is reclassified under this subsection is ranked one level
5 above the ranking under s. 921.0022 of the felony offense
6 committed, and a misdemeanor offense that is reclassified
7 under this subsection is ranked in level 2 of the offense
8 severity ranking chart in s. 921.0022.

9 (6) ~~A Any~~ person who willfully and without
10 authorization fraudulently uses personal identification
11 information concerning an individual who is less than 18 years
12 of age without first obtaining the consent of that individual
13 or of his or her legal guardian commits a felony of the second
14 degree, punishable as provided in s. 775.082, s. 775.083, or
15 s. 775.084.

16 (7) ~~A Any~~ person who is in the relationship of parent
17 or legal guardian, or who otherwise exercises custodial
18 authority over an individual who is less than 18 years of age,
19 who willfully and fraudulently uses personal identification
20 information of that individual commits a felony of the second
21 degree, punishable as provided in s. 775.082, s. 775.083, or
22 s. 775.084.

23 (8)(a) A person who willfully and fraudulently uses,
24 or possesses with intent to fraudulently use, personal
25 identification information concerning a deceased individual
26 commits the offense of fraudulent use or possession with
27 intent to use personal identification information of a
28 deceased individual, a felony of the third degree, punishable
29 as provided in s. 775.082, s. 775.083, or s. 775.084.

30 (b) A person who willfully and fraudulently uses
31 personal identification information concerning a deceased

1 individual commits a felony of the second degree, punishable
2 as provided in s. 775.082, s. 775.083, or s. 775.084, if the
3 pecuniary benefit, the value of the services received, the
4 payment sought to be avoided, or the amount of injury or fraud
5 perpetrated is \$5,000 or more, or if the person fraudulently
6 uses the personal identification information of 10 or more but
7 fewer than 20 deceased individuals. Notwithstanding any other
8 law, the court shall sentence any person convicted of
9 committing the offense described in this paragraph to a
10 mandatory minimum sentence of 3 years' imprisonment.

11 (c) A person who willfully and fraudulently uses
12 personal identification information concerning a deceased
13 individual commits the offense of aggravated fraudulent use of
14 the personal identification information of multiple deceased
15 individuals, a felony of the first degree, punishable as
16 provided in s. 775.082, s. 775.083, or s. 775.084, if the
17 pecuniary benefit, the value of the services received, the
18 payment sought to be avoided, or the amount of injury or fraud
19 perpetrated is \$50,000 or more, or if the person fraudulently
20 uses the personal identification information of 20 or more but
21 fewer than 30 deceased individuals. Notwithstanding any other
22 law, the court shall sentence a person convicted of the
23 offense described in this paragraph to a minimum mandatory
24 sentence of 5 years' imprisonment. If the pecuniary benefit,
25 the value of the services received, the payment sought to be
26 avoided, or the amount of the injury or fraud perpetrated is
27 \$100,000 or more, or if the person fraudulently uses the
28 personal identification information of 30 or more deceased
29 individuals, notwithstanding any other provision of law, the
30 court shall sentence a person convicted of an offense

31

1 described in this paragraph to a mandatory minimum sentence of
2 10 years' imprisonment.

3 (9) A person who willfully and fraudulently creates or
4 uses, or possesses with intent to fraudulently use,
5 counterfeit or fictitious personal identification information
6 concerning a fictitious individual, or concerning a real
7 individual without first obtaining that real individual's
8 consent, with intent to use the counterfeit or fictitious
9 personal identification information for the purpose of
10 committing or facilitating the commission of a fraud on
11 another person, commits the offense of fraudulent creation or
12 use, or possession with intent to fraudulently use,
13 counterfeit or fictitious personal identification information,
14 a felony of the third degree, punishable as provided in s.
15 775.082, s. 775.083, or s. 775.084.

16 (10) A person who commits an offense described in this
17 section and for the purpose of obtaining or using personal
18 identification information misrepresents himself or herself to
19 be a law enforcement officer; an employee or representative of
20 a bank, credit card company, credit counseling company, or
21 credit reporting agency; or a person who wrongfully represents
22 that he or she is seeking to assist the victim with a problem
23 concerning the victim's credit history shall have the offense
24 reclassified as follows:

25 (a) In the case of a misdemeanor, the offense is
26 reclassified as a felony of the third degree.

27 (b) In the case of a felony of the third degree, the
28 offense is reclassified as a felony of the second degree.

29 (c) In the case of a felony of the second degree, the
30 offense is reclassified as a felony of the first degree.

31

1 (d) In the case of a felony of the first degree or a
2 felony of the first degree punishable by a term of
3 imprisonment not exceeding life, the offense is reclassified
4 as a life felony.

5
6 For purposes of sentencing under chapter 921, a felony offense
7 that is reclassified under this subsection is ranked one level
8 above the ranking under s. 921.0022 or s. 921.0023 of the
9 felony offense committed, and a misdemeanor offense that is
10 reclassified under this subsection is ranked in level 2 of the
11 offense severity ranking chart.

12 (11) The prosecutor may move the sentencing court to
13 reduce or suspend the sentence of a person who is convicted of
14 a violation of this section and who provides substantial
15 assistance in the identification, arrest, or conviction of any
16 of that person's accomplices, accessories, coconspirators, or
17 principals or of any other person engaged in fraudulent
18 possession or use of personal identification information. The
19 arresting agency shall be given an opportunity to be heard in
20 aggravation or mitigation in reference to any such motion.
21 Upon good cause shown, the motion may be filed and heard in
22 camera. The judge hearing the motion may reduce or suspend the
23 sentence if the judge finds that the defendant rendered such
24 substantial assistance.

25 (12)(8) This section does not prohibit any lawfully
26 authorized investigative, protective, or intelligence activity
27 of a law enforcement agency of this state or any of its
28 political subdivisions, of any other state or its political
29 subdivisions, or of the Federal Government or its political
30 subdivisions.

31

1 ~~(13)(9)~~(a) In sentencing a defendant convicted of an
2 offense under this section, the court may order that the
3 defendant make restitution under ~~pursuant to~~ s. 775.089 to any
4 victim of the offense. In addition to the victim's
5 out-of-pocket costs, ~~such~~ restitution may include payment of
6 any other costs, including attorney's fees incurred by the
7 victim in clearing the victim's credit history or credit
8 rating, or any costs incurred in connection with any civil or
9 administrative proceeding to satisfy any debt, lien, or other
10 obligation of the victim arising as the result of the actions
11 of the defendant.

12 (b) The sentencing court may issue such orders as are
13 necessary to correct any public record that contains false
14 information given in violation of this section.

15 ~~(14)(10)~~ Prosecutions for violations of this section
16 may be brought on behalf of the state by any state attorney or
17 by the statewide prosecutor.

18 ~~(15)(11)~~ The Legislature finds that, in the absence of
19 evidence to the contrary, the location where a victim gives or
20 fails to give consent to the use of personal identification
21 information is the county where the victim generally resides.

22 ~~(16)(12)~~ Notwithstanding any other provision of law,
23 venue for the prosecution and trial of violations of this
24 section may be commenced and maintained in any county in which
25 an element of the offense occurred, including the county where
26 the victim generally resides.

27 ~~(17)(13)~~ A prosecution of an offense prohibited under
28 subsection (2), subsection (6), or subsection (7) must be
29 commenced within 3 years after the offense occurred. However,
30 a prosecution may be commenced within 1 year after discovery
31 of the offense by an aggrieved party, or by a person who has a

1 legal duty to represent the aggrieved party and who is not a
2 party to the offense, if such prosecution is commenced within
3 5 years after the violation occurred.

4 Section 3. If any provision of this act or its
5 application to any person or circumstance is held invalid, the
6 invalidity does not affect other provisions or applications of
7 the act which can be given effect without the invalid
8 provision or application, and to this end the provisions of
9 this act are severable.

10 Section 4. This act shall take effect July 1, 2005.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31