

CHAMBER ACTION

1 The Justice Council recommends the following:

2
3 **Council/Committee Substitute**

4 Remove the entire bill and insert:

5 A bill to be entitled

6 An act relating to unlawful use of personal identification
7 information; amending s. 817.568, F.S.; including other
8 information within the definition of the term "personal
9 identification information"; defining the term
10 "counterfeit or fictitious personal identification
11 information"; revising criminal penalties relating to the
12 offense of fraudulently using, or possessing with intent
13 to fraudulently use, personal identification information;
14 providing minimum mandatory terms of imprisonment;
15 creating the offenses of willfully and fraudulently using,
16 or possessing with intent to fraudulently use, personal
17 identification information concerning a deceased
18 individual; providing criminal penalties; providing for
19 minimum mandatory terms of imprisonment; creating the
20 offense of willfully and fraudulently creating or using,
21 or possessing with intent to fraudulently use, counterfeit
22 or fictitious personal identification information;
23 providing criminal penalties; providing for

24 reclassification of offenses under certain circumstances;
 25 providing for reduction or suspension of sentences under
 26 certain circumstances; creating s. 817.5681, F.S.;
 27 requiring business persons maintaining computerized data
 28 that includes personal information to provide notice of
 29 breaches of system security under certain circumstances;
 30 providing requirements; providing for administrative
 31 fines; providing exceptions and limitations; authorizing
 32 delays of such disclosures under certain circumstances;
 33 providing definitions; providing for alternative notice
 34 methods; specifying conditions of compliance for persons
 35 maintaining certain alternative notification procedures;
 36 specifying conditions under which notification is not
 37 required; providing requirements for documentation and
 38 maintenance of documentation; providing an administrative
 39 fine for failing to document certain failures to comply;
 40 providing for application of administrative sanctions to
 41 certain persons under certain circumstances; authorizing
 42 the Department of Legal Affairs to institute proceedings
 43 to assess and collect fines; requiring notification of
 44 consumer reporting agencies of breaches of system security
 45 under certain circumstances; providing an effective date.

46
 47 Be It Enacted by the Legislature of the State of Florida:

48
 49 Section 1. Section 817.568, Florida Statutes, is amended
 50 to read:

51 | 817.568 Criminal use of personal identification
52 | information.--

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

54 | (a) "Access device" means any card, plate, code, account
55 | number, electronic serial number, mobile identification number,
56 | personal identification number, or other telecommunications
57 | service, equipment, or instrument identifier, or other means of
58 | account access that can be used, alone or in conjunction with
59 | another access device, to obtain money, goods, services, or any
60 | other thing of value, or that can be used to initiate a transfer
61 | of funds, other than a transfer originated solely by paper
62 | instrument.

63 | (b) "Authorization" means empowerment, permission, or
64 | competence to act.

65 | (c) "Harass" means to engage in conduct directed at a
66 | specific person that is intended to cause substantial emotional
67 | distress to such person and serves no legitimate purpose.

68 | "Harass" does not mean to use personal identification
69 | information for accepted commercial purposes. The term does not
70 | include constitutionally protected conduct such as organized
71 | protests or the use of personal identification information for
72 | accepted commercial purposes.

73 | (d) "Individual" means a single human being and does not
74 | mean a firm, association of individuals, corporation,
75 | partnership, joint venture, sole proprietorship, or any other
76 | entity.

77 | (e) "Person" means a "person" as defined in s. 1.01(3).

78 (f) "Personal identification information" means any name
79 or number that may be used, alone or in conjunction with any
80 other information, to identify a specific individual, including
81 any:

82 1. Name, postal or electronic mail address, telephone
83 number, social security number, date of birth, mother's maiden
84 name, official state-issued or United States-issued driver's
85 license or identification number, alien registration number,
86 government passport number, employer or taxpayer identification
87 number, Medicaid or food stamp account number, ~~or~~ bank account
88 number, ~~or~~ credit or debit card number, or personal
89 identification number or code assigned to the holder of a debit
90 card by the issuer to permit authorized electronic use of such
91 card;

92 2. Unique biometric data, such as fingerprint, voice
93 print, retina or iris image, or other unique physical
94 representation;

95 3. Unique electronic identification number, address, or
96 routing code; ~~or~~

97 4. Medical records;

98 5.4. Telecommunication identifying information or access
99 device; or-

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

102 (g) "Counterfeit or fictitious personal identification
103 information" means any counterfeit, fictitious, or fabricated
104 information in the similitude of the data outlined in paragraph
105 (f) that, although not truthful or accurate, would in context

106 | lead a reasonably prudent person to credit its truthfulness and
 107 | accuracy.

108 | (2)(a) Any person who willfully and without authorization
 109 | fraudulently uses, or possesses with intent to fraudulently use,
 110 | personal identification information concerning an individual
 111 | without first obtaining that individual's consent, commits the
 112 | offense of fraudulent use of personal identification
 113 | information, which is a felony of the third degree, punishable
 114 | as provided in s. 775.082, s. 775.083, or s. 775.084.

115 | (b) Any person who willfully and without authorization
 116 | fraudulently uses personal identification information concerning
 117 | an individual without first obtaining that individual's consent
 118 | commits a felony of the second degree, punishable as provided in
 119 | s. 775.082, s. 775.083, or s. 775.084, if the pecuniary benefit,
 120 | the value of the services received, the payment sought to be
 121 | avoided, or the amount of the injury or fraud perpetrated is
 122 | \$5,000 or more or if the person fraudulently uses the personal
 123 | identification information of 10 or more individuals, but fewer
 124 | than 20 individuals, without their consent. Notwithstanding any
 125 | other provision of law, the court shall sentence any person
 126 | convicted of committing the offense described in this paragraph
 127 | to a mandatory minimum sentence of 3 years' imprisonment.

128 | (c) Any person who willfully and without authorization
 129 | fraudulently uses personal identification information concerning
 130 | an individual without first obtaining that individual's consent
 131 | commits a felony of the first degree, punishable as provided in
 132 | s. 775.082, s. 775.083, or s. 775.084, if the pecuniary benefit,
 133 | the value of the services received, the payment sought to be

HB 481 CS

2005
CS

134 avoided, or the amount of the injury or fraud perpetrated is
 135 \$50,000 or more or if the person fraudulently uses the personal
 136 identification information of 20 or more individuals, but fewer
 137 than 30 individuals, without their consent. Notwithstanding any
 138 other provision of law, the court shall sentence any person
 139 convicted of committing the offense described in this paragraph:

140 ~~1-~~ to a mandatory minimum sentence of 5 years'
 141 imprisonment. If the pecuniary benefit, the value of the
 142 services received, the payment sought to be avoided, or the
 143 amount of the injury or fraud perpetrated is \$100,000 or more,
 144 or if the person fraudulently uses the personal identification
 145 information of 30 or more individuals without their consent,
 146 notwithstanding any other provision of law, the court shall
 147 sentence any person convicted of committing the offense
 148 described in this paragraph

149 ~~2-~~ to a mandatory minimum sentence of 10 years'
 150 imprisonment, ~~if the pecuniary benefit, the value of the~~
 151 ~~services received, the payment sought to be avoided, or the~~
 152 ~~amount of the injury or fraud perpetrated is \$100,000 or more or~~
 153 ~~if the person fraudulently uses the personal identification~~
 154 ~~information of 30 or more individuals without their consent.~~

155 (3) Neither paragraph (2)(b) nor paragraph (2)(c) prevents
 156 a court from imposing a greater sentence of incarceration as
 157 authorized by law. If the minimum mandatory terms of
 158 imprisonment imposed under paragraph (2)(b) or paragraph (2)(c)
 159 exceed the maximum sentences authorized under s. 775.082, s.
 160 775.084, or the Criminal Punishment Code under chapter 921, the
 161 mandatory minimum sentence must be imposed. If the mandatory

162 | minimum terms of imprisonment under paragraph (2)(b) or
 163 | paragraph (2)(c) are less than the sentence that could be
 164 | imposed under s. 775.082, s. 775.084, or the Criminal Punishment
 165 | Code under chapter 921, the sentence imposed by the court must
 166 | include the mandatory minimum term of imprisonment as required
 167 | by paragraph (2)(b) or paragraph (2)(c).

168 | (4) Any person who willfully and without authorization
 169 | possesses, uses, or attempts to use personal identification
 170 | information concerning an individual without first obtaining
 171 | that individual's consent, and who does so for the purpose of
 172 | harassing that individual, commits the offense of harassment by
 173 | use of personal identification information, which is a
 174 | misdemeanor of the first degree, punishable as provided in s.
 175 | 775.082 or s. 775.083.

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

180 | (a) A misdemeanor of the first degree is reclassified as a
 181 | felony of the third degree.

182 | (b) A felony of the third degree is reclassified as a
 183 | felony of the second degree.

184 | (c) A felony of the second degree is reclassified as a
 185 | felony of the first degree.

186 |
 187 | For purposes of sentencing under chapter 921 and incentive gain-
 188 | time eligibility under chapter 944, a felony offense that is
 189 | reclassified under this subsection is ranked one level above the

HB 481 CS

2005
CS

190 ranking under s. 921.0022 of the felony offense committed, and a
 191 misdemeanor offense that is reclassified under this subsection
 192 is ranked in level 2 of the offense severity ranking chart in s.
 193 921.0022.

194 (6) Any person who willfully and without authorization
 195 fraudulently uses personal identification information concerning
 196 an individual who is less than 18 years of age without first
 197 obtaining the consent of that individual or of his or her legal
 198 guardian commits a felony of the second degree, punishable as
 199 provided in s. 775.082, s. 775.083, or s. 775.084.

200 (7) Any person who is in the relationship of parent or
 201 legal guardian, or who otherwise exercises custodial authority
 202 over an individual who is less than 18 years of age, who
 203 willfully and fraudulently uses personal identification
 204 information of that individual commits a felony of the second
 205 degree, punishable as provided in s. 775.082, s. 775.083, or s.
 206 775.084.

207 (8)(a) Any person who willfully and fraudulently uses, or
 208 possesses with intent to fraudulently use, personal
 209 identification information concerning a deceased individual
 210 commits the offense of fraudulent use or possession with intent
 211 to use personal identification information of a deceased
 212 individual, a felony of the third degree, punishable as provided
 213 in s. 775.082, s. 775.083, or s. 775.084.

214 (b) Any person who willfully and fraudulently uses
 215 personal identification information concerning a deceased
 216 individual commits a felony of the second degree, punishable as
 217 provided in s. 775.082, s. 775.083, or s. 775.084, if the

218 pecuniary benefit, the value of the services received, the
 219 payment sought to be avoided, or the amount of injury or fraud
 220 perpetrated is \$5,000 or more, or if the person fraudulently
 221 uses the personal identification information of 10 or more but
 222 fewer than 20 deceased individuals. Notwithstanding any other
 223 provision of law, the court shall sentence any person convicted
 224 of committing the offense described in this paragraph to a
 225 mandatory minimum sentence of 3 years' imprisonment.

226 (c) Any person who willfully and fraudulently uses
 227 personal identification information concerning a deceased
 228 individual commits the offense of aggravated fraudulent use of
 229 the personal identification information of multiple deceased
 230 individuals, a felony of the first degree, punishable as
 231 provided in s. 775.082, s. 775.083, or s. 775.084, if the
 232 pecuniary benefit, the value of the services received, the
 233 payment sought to be avoided, or the amount of injury or fraud
 234 perpetrated is \$50,000 or more, or if the person fraudulently
 235 uses the personal identification information of 20 or more but
 236 fewer than 30 deceased individuals. Notwithstanding any other
 237 provision of law, the court shall sentence any person convicted
 238 of the offense described in this paragraph to a minimum
 239 mandatory sentence of 5 years' imprisonment. If the pecuniary
 240 benefit, the value of the services received, the payment sought
 241 to be avoided, or the amount of the injury or fraud perpetrated
 242 is \$100,000 or more, or if the person fraudulently uses the
 243 personal identification information of 30 or more deceased
 244 individuals, notwithstanding any other provision of law, the
 245 court shall sentence any person convicted of an offense

246 described in this paragraph to a mandatory minimum sentence of
 247 10 years' imprisonment.

248 (9) Any person who willfully and fraudulently creates or
 249 uses, or possesses with intent to fraudulently use, counterfeit
 250 or fictitious personal identification information concerning a
 251 fictitious individual, or concerning a real individual without
 252 first obtaining that real individual's consent, with intent to
 253 use such counterfeit or fictitious personal identification
 254 information for the purpose of committing or facilitating the
 255 commission of a fraud on another person, commits the offense of
 256 fraudulent creation or use, or possession with intent to
 257 fraudulently use, counterfeit or fictitious personal
 258 identification information, a felony of the third degree,
 259 punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

260 (10) Any person who commits an offense described in this
 261 section and for the purpose of obtaining or using personal
 262 identification information misrepresents himself or herself to
 263 be a law enforcement officer; an employee or representative of a
 264 bank, credit card company, credit counseling company, or credit
 265 reporting agency; or any person who wrongfully represents that
 266 he or she is seeking to assist the victim with a problem with
 267 the victim's credit history shall have the offense reclassified
 268 as follows:

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

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

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

275 (d) In the case of a felony of the first degree or a
 276 felony of the first degree punishable by a term of imprisonment
 277 not exceeding life, the offense is reclassified as a life
 278 felony.

279
 280 For purposes of sentencing under chapter 921, a felony offense
 281 that is reclassified under this subsection is ranked one level
 282 above the ranking under s. 921.0022 or s. 921.0023 of the felony
 283 offense committed, and a misdemeanor offense that is
 284 reclassified under this subsection is ranked in level 2 of the
 285 offense severity ranking chart.

286 (11) The prosecutor may move the sentencing court to
 287 reduce or suspend the sentence of any person who is convicted of
 288 a violation of this section and who provides substantial
 289 assistance in the identification, arrest, or conviction of any
 290 of that person's accomplices, accessories, coconspirators, or
 291 principals or of any other person engaged in fraudulent
 292 possession or use of personal identification information. The
 293 arresting agency shall be given an opportunity to be heard in
 294 aggravation or mitigation in reference to any such motion. Upon
 295 good cause shown, the motion may be filed and heard in camera.
 296 The judge hearing the motion may reduce or suspend the sentence
 297 if the judge finds that the defendant rendered such substantial
 298 assistance.

299 (12)~~(8)~~ This section does not prohibit any lawfully
 300 authorized investigative, protective, or intelligence activity

HB 481 CS

2005
CS

301 of a law enforcement agency of this state or any of its
 302 political subdivisions, of any other state or its political
 303 subdivisions, or of the Federal Government or its political
 304 subdivisions.

305 (13)~~(9)~~(a) In sentencing a defendant convicted of an
 306 offense under this section, the court may order that the
 307 defendant make restitution under ~~pursuant to~~ s. 775.089 to any
 308 victim of the offense. In addition to the victim's out-of-pocket
 309 costs, ~~such~~ restitution may include payment of any other costs,
 310 including attorney's fees incurred by the victim in clearing the
 311 victim's credit history or credit rating, or any costs incurred
 312 in connection with any civil or administrative proceeding to
 313 satisfy any debt, lien, or other obligation of the victim
 314 arising as the result of the actions of the defendant.

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

318 (14)~~(10)~~ Prosecutions for violations of this section may
 319 be brought on behalf of the state by any state attorney or by
 320 the statewide prosecutor.

321 (15)~~(11)~~ The Legislature finds that, in the absence of
 322 evidence to the contrary, the location where a victim gives or
 323 fails to give consent to the use of personal identification
 324 information is the county where the victim generally resides.

325 (16)~~(12)~~ Notwithstanding any other provision of law, venue
 326 for the prosecution and trial of violations of this section may
 327 be commenced and maintained in any county in which an element of

HB 481 CS

2005
CS

328 | the offense occurred, including the county where the victim
329 | generally resides.

330 | ~~(17)(13)~~ A prosecution of an offense prohibited under
331 | subsection (2), subsection (6), or subsection (7) must be
332 | commenced within 3 years after the offense occurred. However, a
333 | prosecution may be commenced within 1 year after discovery of
334 | the offense by an aggrieved party, or by a person who has a
335 | legal duty to represent the aggrieved party and who is not a
336 | party to the offense, if such prosecution is commenced within 5
337 | years after the violation occurred.

338 | Section 2. Section 817.5681, Florida Statutes, is created
339 | to read:

340 | 817.5681 Breach of security concerning confidential
341 | personal information in third-party possession; administrative
342 | penalties.--

343 | (1)(a) Any person who conducts business in this state and
344 | maintains computerized data in a system that includes personal
345 | information shall provide notice of any breach of the security
346 | of the system, following a determination of the breach, to any
347 | resident of this state whose unencrypted personal information
348 | was, or is reasonably believed to have been, acquired by an
349 | unauthorized person. The notification shall be made without
350 | unreasonable delay, consistent with the legitimate needs of law
351 | enforcement, as provided in subsection (3) and paragraph
352 | (10)(a), or subject to any measures necessary to determine the
353 | presence, nature, and scope of the breach and restore the
354 | reasonable integrity of the system. Notification must be made no

355 later than 45 days following the determination of the breach
 356 unless otherwise provided in this section.

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

362 1. In the amount of \$1,000 for each day the breach goes
 363 undisclosed for up to 30 days and, thereafter, \$50,000 for each
 364 30-day period or portion thereof for up to 180 days.

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

368 (c) The administrative sanctions for failure to notify
 369 provided in this subsection shall not apply in the case of
 370 personal information in the custody of any governmental agency
 371 or subdivision, unless that governmental agency or subdivision
 372 has entered into a contract with a contractor or third-party
 373 administrator to provide governmental services. In such case,
 374 the contractor or third-party administrator shall be a person to
 375 whom the administrative sanctions provided in this subsection
 376 would apply, although such contractor or third-party
 377 administrator found in violation of the notification
 378 requirements provided in this subsection would not have an
 379 action for contribution or set-off available against the
 380 employing agency or subdivision.

381 (2)(a) Any person who maintains computerized data that
 382 includes personal information on behalf of another business

HB 481 CS

2005
CS

383 entity shall disclose to the business entity for which the
384 information is maintained any breach of the security of the
385 system as soon as practicable, but no later than 10 days
386 following the determination, if the personal information was, or
387 is reasonably believed to have been, acquired by an unauthorized
388 person. The person who maintains the data on behalf of another
389 business entity and the business entity on whose behalf the data
390 is maintained may agree who will provide the notice, if any is
391 required, as provided in paragraph (1)(a), provided only a
392 single notice for each breach of the security of the system
393 shall be required. If agreement regarding notification cannot be
394 reached, the person who has the direct business relationship
395 with the resident of this state shall be subject to the
396 provisions of paragraph (1)(a).

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

402 1. In the amount of \$1,000 for each day the breach goes
403 undisclosed for up to 30 days and, thereafter, \$50,000 for each
404 30-day period or portion thereof for up to 180 days.

405 2. If disclosure is not made within 180 days, any person
406 required to make disclosures under paragraph (a) who fails to do
407 so is subject to an administrative fine of up to \$500,000.

408 (c) The administrative sanctions for nondisclosure
409 provided in this subsection shall not apply in the case of
410 personal information in the custody of any governmental agency

411 or subdivision unless that governmental agency or subdivision
 412 has entered into a contract with a contractor or third-party
 413 administrator to provide governmental services. In such case,
 414 the contractor or third-party administrator shall be a person to
 415 whom the administrative sanctions provided in this subsection
 416 would apply, although such contractor or third-party
 417 administrator found in violation of the nondisclosure
 418 restrictions in this subsection would not have an action for
 419 contribution or set-off available against the employing agency
 420 or subdivision.

421 (3) The notification required by this section may be
 422 delayed upon a request by law enforcement if a law enforcement
 423 agency determines that the notification will impede a criminal
 424 investigation. The notification time period required by this
 425 section shall commence after the person receives notice from the
 426 law enforcement agency that the notification will not compromise
 427 the investigation.

428 (4) For purposes of this section, the terms "breach" and
 429 "breach of the security of the system" mean unlawful and
 430 unauthorized acquisition of computerized data that materially
 431 compromises the security, confidentiality, or integrity of
 432 personal information maintained by the person. Good faith
 433 acquisition of personal information by an employee or agent of
 434 the person is not a breach or breach of the security of the
 435 system, provided the information is not used for a purpose
 436 unrelated to the business or subject to further unauthorized
 437 use.

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

443 (a) Social security number.

444 (b) Driver's license number or Florida Identification Card
 445 number.

446 (c) Account number, credit card number, or debit card
 447 number, in combination with any required security code, access
 448 code, or password that would permit access to an individual's
 449 financial account.

450
 451 For purposes of this section, the term "personal information"
 452 does not include publicly available information that is lawfully
 453 made available to the general public from federal, state, or
 454 local government records or widely distributed media.

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

457 (a) Written notice;

458 (b) Electronic notice, if the notice provided is
 459 consistent with the provisions regarding electronic records and
 460 signatures set forth in 15 U.S.C. s. 7001 or if the person or
 461 business providing the notice has a valid email address for the
 462 subject person and the subject person has agreed to accept
 463 communications electronically; or

464 (c) Substitute notice, if the person demonstrates that the
 465 cost of providing notice would exceed \$250,000, the affected

466 class of subject persons to be notified exceeds 500,000, or the
 467 person does not have sufficient contact information. Substitute
 468 notice shall consist of all of the following:

469 1. Electronic mail or email notice when the person has an
 470 electronic mail or email address for the subject persons.

471 2. Conspicuous posting of the notice on the web page of
 472 the person, if the person maintains a web page.

473 3. Notification to major statewide media.

474 (7) For purposes of this section, the term "unauthorized
 475 person" means any person who does not have permission from, or a
 476 password issued by, the person who stores the computerized data
 477 to acquire such data, but does not include any individual to
 478 whom the personal information pertains.

479 (8) For purposes of this section, the term "person" means
 480 a person as defined in s. 1.01(3). For purposes of this section,
 481 the State of Florida, as well as any of its agencies or
 482 political subdivisions, and any of the agencies of its political
 483 subdivisions, constitutes a person.

484 (9) Notwithstanding subsection (6), a person who
 485 maintains:

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

490 (b) A notification procedure pursuant to the rules,
 491 regulations, procedures, or guidelines established by the
 492 person's primary or functional federal regulator,

493

494 shall be deemed to be in compliance with the notification
 495 requirements of this section if the person notifies subject
 496 persons in accordance with the person's policies or the rules,
 497 regulations, procedures, or guidelines established by the
 498 primary or functional federal regulator in the event of a breach
 499 of security of the system.

500 (10)(a) Notwithstanding subsection (2), notification is
 501 not required if, after an appropriate investigation or after
 502 consultation with relevant federal, state, and local agencies
 503 responsible for law enforcement, the person reasonably
 504 determines that the breach has not and will not likely result in
 505 harm to the individuals whose personal information has been
 506 acquired and accessed. Such a determination must be documented
 507 in writing and the documentation must be maintained for 5 years.

508 (b) Any person required to document a failure to notify
 509 affected persons who fails to document the failure as required
 510 in this subsection or who, if documentation was created, fails
 511 to maintain the documentation for the full 5 years as required
 512 in this subsection is liable for an administrative fine in the
 513 amount of up to \$50,000 for such failure.

514 (c) The administrative sanctions outlined in this
 515 subsection shall not apply in the case of personal information
 516 in the custody of any governmental agency or subdivision, unless
 517 that governmental agency or subdivision has entered into a
 518 contract with a contractor or third-party administrator to
 519 provide governmental services. In such case the contractor or
 520 third-party administrator shall be a person to whom the
 521 administrative sanctions outlined in this subsection would

HB 481 CS

2005
CS

522 apply, although such contractor or third-party administrator
523 found in violation of the documentation and maintenance of
524 documentation requirements in this subsection would not have an
525 action for contribution or set-off available against the
526 employing agency or subdivision.

527 (11) The Department of Legal Affairs may institute
528 proceedings to assess and collect the fines provided in this
529 section.

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

537 Section 3. This act shall take effect July 1, 2005.