

CHAMBER ACTION

1 The Business Regulation Committee 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; providing an effective date.

44

45 Be It Enacted by the Legislature of the State of Florida:

46

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

49 817.568 Criminal use of personal identification  
 50 information.--

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

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

61 (b) "Authorization" means empowerment, permission, or  
 62 competence to act.

63 (c) "Harass" means to engage in conduct directed at a  
 64 specific person that is intended to cause substantial emotional  
 65 distress to such person and serves no legitimate purpose.  
 66 "Harass" does not mean to use personal identification  
 67 information for accepted commercial purposes. The term does not  
 68 include constitutionally protected conduct such as organized  
 69 protests or the use of personal identification information for  
 70 accepted commercial purposes.

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

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

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

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

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

93           3. Unique electronic identification number, address, or  
 94 routing code; ~~or~~

95           4. Medical records;

96           ~~5.4.~~ Telecommunication identifying information or access  
 97 device; ~~or.~~

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

100           (g) "Counterfeit or fictitious personal identification  
 101 information" means any counterfeit, fictitious, or fabricated  
 102 information in the similitude of the data outlined in paragraph  
 103 (f) that, although not truthful or accurate, would in context  
 104 lead a reasonably prudent person to credit its truthfulness and  
 105 accuracy.

106           (2)(a) Any person who willfully and without authorization  
 107 fraudulently uses, or possesses with intent to fraudulently use,

HB 481 CS

2005  
CS

108 | personal identification information concerning an individual  
 109 | without first obtaining that individual's consent, commits the  
 110 | offense of fraudulent use of personal identification  
 111 | information, which is a felony of the third degree, punishable  
 112 | as provided in s. 775.082, s. 775.083, or s. 775.084.

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

126 |       (c) Any person who willfully and without authorization  
 127 | fraudulently uses personal identification information concerning  
 128 | an individual without first obtaining that individual's consent  
 129 | commits a felony of the first degree, punishable as provided in  
 130 | s. 775.082, s. 775.083, or s. 775.084, if the pecuniary benefit,  
 131 | the value of the services received, the payment sought to be  
 132 | avoided, or the amount of the injury or fraud perpetrated is  
 133 | \$50,000 or more or if the person fraudulently uses the personal  
 134 | identification information of 20 or more individuals, but fewer  
 135 | than 30 individuals, without their consent. Notwithstanding any

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

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

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

164 include the mandatory minimum term of imprisonment as required  
165 by paragraph (2)(b) or paragraph (2)(c).

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

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

178 (a) A misdemeanor of the first degree is reclassified as a  
179 felony of the third degree.

180 (b) A felony of the third degree is reclassified as a  
181 felony of the second degree.

182 (c) A felony of the second degree is reclassified as a  
183 felony of the first degree.

184

185 For purposes of sentencing under chapter 921 and incentive gain-  
186 time eligibility under chapter 944, a felony offense that is  
187 reclassified under this subsection is ranked one level above the  
188 ranking under s. 921.0022 of the felony offense committed, and a  
189 misdemeanor offense that is reclassified under this subsection  
190 is ranked in level 2 of the offense severity ranking chart in s.  
191 921.0022.

HB 481 CS

2005  
CS

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

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

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

212 (b) Any person who willfully and fraudulently uses  
 213 personal identification information concerning a deceased  
 214 individual commits a felony of the second degree, punishable as  
 215 provided in s. 775.082, s. 775.083, or s. 775.084, if the  
 216 pecuniary benefit, the value of the services received, the  
 217 payment sought to be avoided, or the amount of injury or fraud  
 218 perpetrated is \$5,000 or more, or if the person fraudulently  
 219 uses the personal identification information of 10 or more but



220 fewer than 20 deceased individuals. Notwithstanding any other  
 221 provision of law, the court shall sentence any person convicted  
 222 of committing the offense described in this paragraph to a  
 223 mandatory minimum sentence of 3 years' imprisonment.

224 (c) Any person who willfully and fraudulently uses  
 225 personal identification information concerning a deceased  
 226 individual commits the offense of aggravated fraudulent use of  
 227 the personal identification information of multiple deceased  
 228 individuals, a felony of the first degree, punishable as  
 229 provided in s. 775.082, s. 775.083, or s. 775.084, if the  
 230 pecuniary benefit, the value of the services received, the  
 231 payment sought to be avoided, or the amount of injury or fraud  
 232 perpetrated is \$50,000 or more, or if the person fraudulently  
 233 uses the personal identification information of 20 or more but  
 234 fewer than 30 deceased individuals. Notwithstanding any other  
 235 provision of law, the court shall sentence any person convicted  
 236 of the offense described in this paragraph to a minimum  
 237 mandatory sentence of 5 years' imprisonment. If the pecuniary  
 238 benefit, the value of the services received, the payment sought  
 239 to be avoided, or the amount of the injury or fraud perpetrated  
 240 is \$100,000 or more, or if the person fraudulently uses the  
 241 personal identification information of 30 or more deceased  
 242 individuals, notwithstanding any other provision of law, the  
 243 court shall sentence any person convicted of an offense  
 244 described in this paragraph to a mandatory minimum sentence of  
 245 10 years' imprisonment.

246 (9) Any person who willfully and fraudulently creates or  
 247 uses, or possesses with intent to fraudulently use, counterfeit

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

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

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

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

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

273 (d) In the case of a felony of the first degree or a  
 274 felony of the first degree punishable by a term of imprisonment

275 not exceeding life, the offense is reclassified as a life  
 276 felony.

277  
 278 For purposes of sentencing under chapter 921, a felony offense  
 279 that is reclassified under this subsection is ranked one level  
 280 above the ranking under s. 921.0022 or s. 921.0023 of the felony  
 281 offense committed, and a misdemeanor offense that is  
 282 reclassified under this subsection is ranked in level 2 of the  
 283 offense severity ranking chart.

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

297 (12)(8) This section does not prohibit any lawfully  
 298 authorized investigative, protective, or intelligence activity  
 299 of a law enforcement agency of this state or any of its  
 300 political subdivisions, of any other state or its political  
 301 subdivisions, or of the Federal Government or its political  
 302 subdivisions.

303        (13)~~(9)~~(a) In sentencing a defendant convicted of an  
 304 offense under this section, the court may order that the  
 305 defendant make restitution under ~~pursuant to~~ s. 775.089 to any  
 306 victim of the offense. In addition to the victim's out-of-pocket  
 307 costs, ~~such~~ restitution may include payment of any other costs,  
 308 including attorney's fees incurred by the victim in clearing the  
 309 victim's credit history or credit rating, or any costs incurred  
 310 in connection with any civil or administrative proceeding to  
 311 satisfy any debt, lien, or other obligation of the victim  
 312 arising as the result of the actions of the defendant.

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

316        (14)~~(10)~~ Prosecutions for violations of this section may  
 317 be brought on behalf of the state by any state attorney or by  
 318 the statewide prosecutor.

319        (15)~~(11)~~ The Legislature finds that, in the absence of  
 320 evidence to the contrary, the location where a victim gives or  
 321 fails to give consent to the use of personal identification  
 322 information is the county where the victim generally resides.

323        (16)~~(12)~~ Notwithstanding any other provision of law, venue  
 324 for the prosecution and trial of violations of this section may  
 325 be commenced and maintained in any county in which an element of  
 326 the offense occurred, including the county where the victim  
 327 generally resides.

328        (17)~~(13)~~ A prosecution of an offense prohibited under  
 329 subsection (2), subsection (6), or subsection (7) must be  
 330 commenced within 3 years after the offense occurred. However, a

331 prosecution may be commenced within 1 year after discovery of  
 332 the offense by an aggrieved party, or by a person who has a  
 333 legal duty to represent the aggrieved party and who is not a  
 334 party to the offense, if such prosecution is commenced within 5  
 335 years after the violation occurred.

336 Section 2. Section 817.5681, Florida Statutes, is created  
 337 to read:

338 817.5681 Breach of security concerning confidential  
 339 personal information in third-party possession; administrative  
 340 penalties.--

341 (1)(a) Any person who conducts business in this state and  
 342 maintains computerized data in a system that includes personal  
 343 information shall provide notice of any breach of the security  
 344 of the system, following a determination of the breach, to any  
 345 resident of this state whose unencrypted personal information  
 346 was, or is reasonably believed to have been, acquired by an  
 347 unauthorized person. The notification shall be made without  
 348 unreasonable delay, consistent with the legitimate needs of law  
 349 enforcement, as provided in subsection (3) and paragraph  
 350 (10)(a), or subject to any measures necessary to determine the  
 351 presence, nature, and scope of the breach and restore the  
 352 reasonable integrity of the system. Notification must be made no  
 353 later than 45 days following the determination of the breach  
 354 unless otherwise provided in this section.

355 (b) Any person required to make notification under  
 356 paragraph (a) who fails to do so within 45 days following the  
 357 determination of a breach or receipt of notice from law

HB 481 CS

2005  
CS

358 enforcement as provided in subsection (3) is liable for an  
359 administrative fine not to exceed \$500,000, as follows:

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

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

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

379 (2)(a) Any person who maintains computerized data that  
380 includes personal information on behalf of another business  
381 entity shall disclose to the business entity for which the  
382 information is maintained any breach of the security of the  
383 system as soon as practicable, but no later than 10 days  
384 following the determination, if the personal information was, or  
385 is reasonably believed to have been, acquired by an unauthorized

HB 481 CS

2005  
CS

386 person. The person who maintains the data on behalf of another  
387 business entity and the business entity on whose behalf the data  
388 is maintained may agree who will provide the notice, if any is  
389 required, as provided in paragraph (1)(a), provided only a  
390 single notice for each breach of the security of the system  
391 shall be required. If agreement regarding notification cannot be  
392 reached, the person who has the direct business relationship  
393 with the resident of this state shall be subject to the  
394 provisions of paragraph (1)(a).

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

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

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

406 (c) The administrative sanctions for nondisclosure  
407 provided in this subsection shall not apply in the case of  
408 personal information in the custody of any governmental agency  
409 or subdivision unless that governmental agency or subdivision  
410 has entered into a contract with a contractor or third-party  
411 administrator to provide governmental services. In such case,  
412 the contractor or third-party administrator shall be a person to  
413 whom the administrative sanctions provided in this subsection

414 would apply, although such contractor or third-party  
 415 administrator found in violation of the nondisclosure  
 416 restrictions in this subsection would not have an action for  
 417 contribution or set-off available against the employing agency  
 418 or subdivision.

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

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

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

441 (a) Social security number.



HB 481 CS

2005  
CS

442 (b) Driver's license number or Florida Identification Card  
443 number.

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

448  
449 For purposes of this section, the term "personal information"  
450 does not include publicly available information that is lawfully  
451 made available to the general public from federal, state, or  
452 local government records or widely distributed media.

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

455 (a) Written notice;

456 (b) Electronic notice, if the notice provided is  
457 consistent with the provisions regarding electronic records and  
458 signatures set forth in 15 U.S.C. s. 7001; or

459 (c) Substitute notice, if the person demonstrates that the  
460 cost of providing notice would exceed \$250,000, the affected  
461 class of subject persons to be notified exceeds 500,000, or the  
462 person does not have sufficient contact information. Substitute  
463 notice shall consist of all of the following:

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

466 2. Conspicuous posting of the notice on the web page of  
467 the person, if the person maintains a web page.

468 3. Notification to major statewide media.

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

474        (8) For purposes of this section, the term "person" means  
 475 a person as defined in s. 1.01(3). For purposes of this section,  
 476 the State of Florida, as well as any of its agencies or  
 477 political subdivisions, and any of the agencies of its political  
 478 subdivisions, constitutes a person.

479        (9) Notwithstanding subsection (6), a person who  
 480 maintains:

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

485        (b) A notification procedure pursuant to the rules,  
 486 regulations, procedures, or guidelines established by the  
 487 person's primary or functional federal regulator,  
 488  
 489 shall be deemed to be in compliance with the notification  
 490 requirements of this section if the person notifies subject  
 491 persons in accordance with the person's policies or the rules,  
 492 regulations, procedures, or guidelines established by the  
 493 primary or functional federal regulator in the event of a breach  
 494 of security of the system.

495        (10)(a) Notwithstanding subsection (2), notification is  
 496 not required if, after an appropriate investigation and after

497 consultation with relevant federal, state, and local agencies  
 498 responsible for law enforcement, the person reasonably  
 499 determines that the breach has not and will not likely result in  
 500 harm to the individuals whose personal information has been  
 501 acquired and accessed. Such a determination must be documented  
 502 in writing and the documentation must be maintained for 5 years.

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

509 (c) The administrative sanctions outlined in this  
 510 subsection shall not apply in the case of personal information  
 511 in the custody of any governmental agency or subdivision, unless  
 512 that governmental agency or subdivision has entered into a  
 513 contract with a contractor or third-party administrator to  
 514 provide governmental services. In such case the contractor or  
 515 third-party administrator shall be a person to whom the  
 516 administrative sanctions outlined in this subsection would  
 517 apply, although such contractor or third-party administrator  
 518 found in violation of the documentation and maintenance of  
 519 documentation requirements in this subsection would not have an  
 520 action for contribution or set-off available against the  
 521 employing agency or subdivision.

522 (11) The Department of Legal Affairs may institute  
 523 proceedings to assess and collect the fines provided in this  
 524 section.

HB 481 CS

2005  
CS

525

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