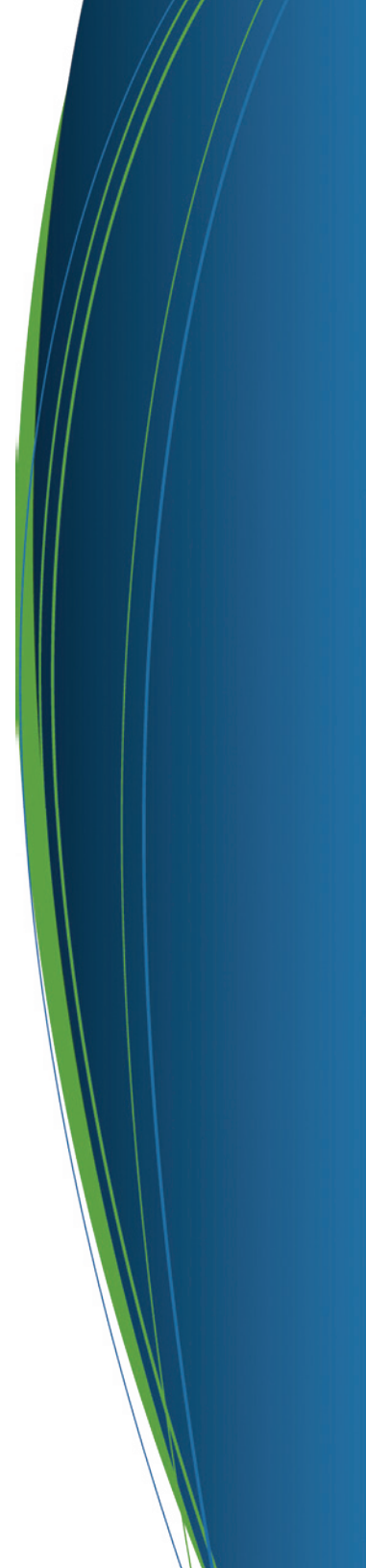


INTERSECTIONS DATA BREACH CONSUMER NOTIFICATION GUIDE



JANUARY 2012



Section I		
Introduction4	
Section II		
State and Territory Regulations		
Alaska5	
Arizona7	
Arkansas9	
California	11	
Colorado	17	
Connecticut	19	
Delaware	23	
District of Columbia	25	
Florida	27	
Georgia	29	
Hawaii	31	
Idaho	33	
Illinois	35	
Indiana	37	
Iowa	39	
Kansas	41	
Louisiana	43	
Maine	45	
Maryland	47	
Massachusetts	49	
Michigan	51	
Minnesota	53	
Mississippi	55	
Missouri	57	
Montana	59	
Nebraska	61	
Nevada	63	
New Hampshire	65	
New Jersey	67	
New York	69	
North Carolina	73	
North Dakota	75	
Ohio	77	
Oklahoma	79	
Oregon	81	
		Pennsylvania 83
		Puerto Rico 85
		Rhode Island 87
		South Carolina 89
		Tennessee 91
		Texas 93
		Utah 95
		Vermont 97
		Virgin Islands 99
		Virginia 101
		Washington 103
		West Virginia 105
		Wisconsin 107
		Wyoming 109
		Section III
		Federal Rules and Guidelines
		Office of Management and
		Budget (OMB) 111
		Interagency Guidance on Response
		Programs for Unauthorized Access
		to Customer Information and
		Customer Notice 113
		FTC Health Breach
		Notification Rule 115
		HHS Breach Notification for Unsecured
		Health Information 117
		Section IV
		Additional Law Enforcement Contacts
		National 120
		Alabama 120
		Kentucky 120
		New Mexico 120
		South Dakota 120
		American Samoa 120
		Guam 120
		Northern Mariana Islands 120
		Section V
		About Intersections 121

INTRODUCTION

One of the leading topics continuing to be discussed by both state and federal lawmakers, is privacy protection, including data breach notification. Currently 46 states, the District of Columbia, Puerto Rico and the Virgin Islands all have passed data breach notification regulations. The number of laws will continue to grow in the coming year and there continues to be much discussion regarding federal regulation as well.

These requirements are designed to dictate who companies notify and the means in which they notify consumers in the event of a data breach. With so many state laws to consider, companies who conduct business across the country can easily become confused and find themselves with difficulties especially considering the pressure they are under to get notices out to consumers quickly. A large data breach impacting consumers across multiple jurisdictions often can require a company to understand and comply with many, if not all laws which frequently conflict and contain subtle and not so subtle differences.

The purpose of this “Intersections Data Breach Consumer Notification Guide” is to help companies better understand what states have data breach notification laws and, more specifically, what those laws require. Armed with this knowledge, companies can better plan for and react to the unfortunate event of a data breach. To find out the best ways to achieve a state of data breach readiness, please refer to the “Intersections’ Seven Steps to Data Breach Readiness Guide”.

Intersections Inc. has been a leader in the fight against identity theft for over a decade. We have protected the identities of more than 34 million consumers and helped tens of thousands of individuals recover after a verified case of identity theft. We understand the harm that a corporate breach event can cause for companies and their customers, which is why we offer a full line of breach response products and services to provide both peace of mind and a compelling brand experience.



THE INFORMATION, DATA AND OTHER CONTENT IN THIS SUMMARY SHOULD NOT BE CONSIDERED AS LEGAL ADVICE. IT IS PROVIDED TO YOU “AS IS” AND WITH NO WARRANTY WHATSOEVER. SPECIFICALLY, INTERSECTIONS INC. (“INTERSECTIONS”) MAKES NO WARRANTY REGARDING THE ACCURACY OR RELIABILITY OF ANY INFORMATION, DATA OR OTHER CONTENT PROVIDED IN THIS SUMMARY AND UNDER NO CIRCUMSTANCES WILL INTERSECTIONS BE LIABLE FOR ANY LOSS OR DAMAGE CAUSED BY YOUR RELIANCE ON THE INFORMATION, DATA OR OTHER CONTENT CONTAINED IN THIS SUMMARY.

IT IS YOUR RESPONSIBILITY TO EVALUATE THE ACCURACY, COMPLETENESS AND USEFULNESS OF ANY INFORMATION, DATA OR OTHER CONTENT PROVIDED IN THIS SUMMARY. PLEASE SEEK THE ADVICE OF A LEGAL PROFESSIONAL, AS APPROPRIATE, REGARDING THE EVALUATION OF ANY SPECIFIC INFORMATION, DATA OR OTHER CONTENT PROVIDED IN THIS SUMMARY.

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/09

What is a breach:

Unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information, including acquisition by: photocopying; facsimile; other paper-based method; a device, including a computer that can read, write, or store information that is represented in numerical form; and other methods not identified.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or state identification number; (3) account, credit or debit card number; (4) personal code to access an account including a security code, access code, personal identification number or password; or (5) passwords, personal identification numbers, or other access codes for financial accounts in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- An information collector that owns or licenses personal information in any form.
- An information recipient that maintains personal information must notify and cooperate with the information distributor that owns or licenses the personal information.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient manner possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it will no longer interfere with the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if the person's primary method of communication is electronic or if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$150,000 or number of persons exceeds 300,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after investigation and written notice to the Attorney General, there is no reasonable likelihood that harm has resulted or will result.
- The determination must be documented in writing for five years.

STATUTORY:

- Credit reporting agency notice provision does not apply if the information collector is subject to the Gramm-Leach-Bliley Act (GLB).

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of an information collector for a legitimate purpose if the employee or agent does not use the personal information for a purpose unrelated to a legitimate purpose or make further unauthorized disclosure.

ENCRYPTION:

- Notice is not required if the personal information was encrypted or redacted and the encryption key has not been accessed or acquired.

STATUTE CITATION

Alaska Stat. §§ 45.48.010 through 45.48.090

Original bill text:

http://www.legis.state.ak.us/basis/get_bill_text.asp?hsid=HB0065Z&session=25

or

Statutory code:

<http://www.legis.state.ak.us/basis/folioproxy.asp?url=http://www.jnu01.legis.state.ak.us/cgi-bin/folioisa.dll/stattx08/query=45!2E48/doc/{@19883}>

ATTORNEY GENERAL

John Burns, Esquire
Attorney General of Alaska
Diamond Courthouse
P.O. Box 110300
Juneau, AK 99811
907-465-2133
attorney.general@alaska.gov

FBI

Anchorage
101 East Sixth Avenue
Anchorage, Alaska 99501-2524
<http://anchorage.fbi.gov>
907-276-4441

SECRET SERVICE

Anchorage
907-271-5148

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 12/31/06

What is a breach:

Unauthorized acquisition and access to unencrypted or unredacted computerized data.

When is notice required:

- Computerized data containing personal information: unencrypted or unredacted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) financial account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A person that owns or licenses computerized data.
- A person that maintains computerized data must notify and cooperate with the owner or licensee.

Who has to be notified:

- The individual.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient manner possible and without unreasonable delay.
- Notification may be delayed if law enforcement agency advises that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it will not compromise the investigation.
- Notification may be delayed to determine the nature and scope of the breach, to identify individuals affected, or to restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if the person's primary method of communication is electronic or if electronic notice is consistent with E-Sign requirements.
- Telephonic.
- Substitute notice may be done if cost of providing notice exceeds \$50,000 or number of persons exceeds 100,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if the acquisition is not reasonably likely to cause substantial economic loss.
- Notice is not required if, after a reasonable investigation, there is a determination that a breach of the security of the system has not occurred or is not reasonably likely to occur.

STATUTORY:

- Exemptions from certain requirements for entities subject to the Gramm-Leach-Bliley Act (GLB) Title V and for Health Insurance Portability and Accountability Act (HIPAA) covered entities.
- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are in compliance with rules, regulations, procedures, guidance or guidelines established by the primary or functional federal regulator.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person maintains their own notification procedures; and if the person notifies the affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition by an employee or agent of the person if the personal information is not used for an unrelated purpose or subject to further willful unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

ENCRYPTION:

- Notice is not required if the personal information was encrypted or redacted.

STATUTE CITATION

Ariz. Rev. Stat. Ann. 44-7501(h)
[Original bill text:
<http://www.azleg.gov/legtext/47leg/2r/bills/sb1338s.htm?printformat=yes>](http://www.azleg.gov/legtext/47leg/2r/bills/sb1338s.htm?printformat=yes)

or

[Statutory code:
<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/44/07501.htm&Title=44>](http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/44/07501.htm&Title=44)

ATTORNEY GENERAL

Tom Horne, Esquire
 Attorney General of Arizona
 1275 W. Washington Street
 Phoenix, AZ 85007
 602-542-4266

FBI

Phoenix
 201 East Indianola Avenue
 Phoenix, Arizona 85012-2080
<http://phoenix.fbi.gov>
 602-279-5511

SECRET SERVICE

Phoenix
 602-640-5580
 Tucson
 520-622-6822

SUMMARY OF LAW - EFFECTIVE DATE - 8/12/05

What is a breach:

Unencrypted or unredacted personal information that was, or is reasonably believed to have been, acquired by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted or unredacted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) financial account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account; and (4) medical information (any individually identifiable information regarding the individual's medical history or medical treatment or diagnosis by a health care professional).

Who has to notify:

- A person that owns or licenses computerized data.
- A person that maintains computerized data must notify the owner or licensee.

Who has to be notified:

- The individual.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time and manner possible and without unreasonable delay.
- Notification may be delayed for legitimate needs of law enforcement if notification would impede a criminal investigation. Notification is required after the law enforcement agency determines that it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after investigation, a business determines that there is no reasonable likelihood of harm.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are in compliance with or regulated by state or federal law that provides greater protection and at least as thorough disclosure requirements.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person or business maintains its own notification procedures consistent with the timing requirements of state law; and if the person or business notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure.

ENCRYPTION:

- Notice is not required if the personal information was encrypted.

STATUTE CITATION

Ark. Code § 4-110-105 (2006)

Original bill text:

<ftp://www.arkleg.state.ar.us/acts/2005/public/act1526.pdf>

or

Statutory code:

<http://www.lexisnexis.com/hottopics/arcod/Default.asp> (Title 4 > Subtitle 7 > Chapter 110 > 4-110-105. Disclosure of security breaches.)

ATTORNEY GENERAL

Dustin McDaniel, Esquire
Attorney General of Arkansas
200 Tower Building
323 Center Street
Little Rock, AR 72201-2610
800-482-8982

FBI

Little Rock
24 Shackelford West Boulevard
Little Rock, Arkansas 72211-3755
<http://littlerock.fbi.gov>
501-221-9100

SECRET SERVICE

Little Rock
501-324-6241

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/03, AMENDMENTS EFFECTIVE - 9/1/12

SECTION 1798.82:

What is a breach:

Unencrypted or unredacted computerized personal information that was, or is reasonably believed to have been, acquired by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted or unredacted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account; (4) medical information; or (5) health information.
- For purposes of this section, “medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

Who has to notify:

- A person that owns or licenses computerized data.
- A person that maintains computerized data must notify the owner or licensee.
- A state guidance document distinguishes between data owners and data custodians, providing that data owners should require custodians to notify owners upon detection of an incident. See www.privacy.ca.gov/recommendations/secbreach.pdf.

Who has to be notified:

- The individual.
- Regulatory/law enforcement notice not specifically addressed.
- State guidance document recommends notifying law enforcement and consumer reporting agencies. See www.privacy.ca.gov/recommendations/secbreach.pdf.
- Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system must also submit a single electronic sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General.

Required contents of notice:

- Written in plain language.
- The name and contact information of the reporting person or business.

- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred.
- The date of the notice.
- Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
- A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

At the discretion of the person or business, the security breach notification may also include any of the following:

- Information about what the person or business has done to protect individuals whose information has been breached.
- Advice on steps that the person whose information has been breached may take to protect himself or herself.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.
- Notification may be delayed for legitimate needs of law enforcement if notification would impede a criminal investigation.
- State guidance document recommends notifying individuals within 10 business days. See www.privacy.ca.gov/recommendations/secbreach.pdf.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email (when available); (ii) web site posting; and (iii) notice to major statewide media and the Office of Privacy Protection within the State and Consumer Services Agency.

SECTION 1798.29 (STATE AGENCIES):

Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

WHEN IS NOTICE NOT REQUIRED**EXISTING POLICY:**

- Notice is not required if a person or business maintains its own notification procedures consistent with the timing requirements of state law; and if the person or business notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of a person or business if the personal information is not otherwise used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of records of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the personal information was encrypted.

STATUTORY:

- Notice is not required if an entity is covered under HIPAA and if the entity has complied with Section 13402(f) of the HITECH Act.

STATUTE CITATION

Cal. Civ. Code title 1.81 § 1798.82

Original bill text:

http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_1251-1300/ab_1298_bill_20071014_chaptered.pdf

Amended by S.B. 24:

http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0001-0050/sb_24_bill_20110819_enrolled.pdf

Cal. Civ. Code title 1.8 § 1798.29

Original bill text:

http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_1251-1300/ab_1298_bill_20071014_chaptered.pdf

Amended by S.B. 24:

http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0001-0050/sb_24_bill_20110819_enrolled.pdf

California Data Breach Guidance Document:

http://www.privacy.ca.gov/res/docs/pdf/COPP_Breach_Reco_Practices_6-09.pdf

(See Appendix 3 and Appendix 4)

ATTORNEY GENERAL

Kamala Harris, Esquire
Attorney General of California

1300 I Street, Suite 1740
Sacramento, CA 95814
916-445-9555

FBI

Los Angeles

11000 Wilshire Blvd.
Suite 1700, FOB
Los Angeles, California 90024-3672
<http://losangeles.fbi.gov>
310-477-6565

Sacramento

4500 Orange Grove Ave.
Sacramento, California 95841-4205
<http://sacramento.fbi.gov>
916-481-9110

San Diego

Federal Office Building
9797 Aero Drive
San Diego, California 92123-1800
<http://sandiego.fbi.gov>
858-565-1255

San Francisco

450 Golden Gate Avenue, 13th. Floor
San Francisco, California 94102-9523
<http://sanfrancisco.fbi.gov>
415-553-7400

SECRET SERVICE

Fresno
559-487-5204

Riverside
951-276-6781

Sacramento
916-325-5481

San Diego
619-557-5640

San Jose
408-535-5288

Santa Ana
714-246-8257

Ventura
805-383-5745

Electronic Crimes Task Force
Los Angeles

213-894-4830
Email: Lax.ectfreports@usss.dhs.gov

Electronic Crimes Task Force
San Francisco

415-744-9026
Email: sfoectf@einformation.usss.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/10 - AMDTS IN EFFECT ON 9/29/10
SECTION 1280.15 (CLINICS, HEALTH FACILITIES, HOME HEALTH AGENCIES, AND HOSPICES):

What is a breach:

“Unauthorized” means the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1 of the Civil Code) or any other statute or regulation governing the lawful access, use, or disclosure of medical information.

When is notice required:

- “Medical information” means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient’s medical history, mental or physical condition, or treatment. “Individually identifiable” means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual’s identity.

Who has to notify:

- A clinic, health facility, home health agency, or hospice

Who has to be notified:

- The State Department of Public Health; and
- The affected patient or the patient’s representative at the last known address.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- No later than 5 business days after the unlawful or unauthorized access, use, or disclosure of a patient’s medical information has been detected.
- Notification may be delayed beyond 5 business days if a law enforcement agency or official provides a written or oral statement that compliance with the reporting requirements would be likely to impede the law enforcement agency’s investigation and specifies a date upon which the delay shall end, not to exceed 60 days after a written request is made, or 30 days after an oral request is made. A law enforcement agency or official may request an extension of a delay based upon a written declaration (1) that there exists a bona fide, ongoing, significant criminal investigation of serious wrongdoing, (2) that notification of patients will undermine the law enforcement agency’s investigation, and (3) that specifies a date upon which the delay shall end, not to exceed 60 days after the end of the original delay period. If the statement of the law enforcement agency or official is made orally, then the clinic, health facility, home health agency, or hospice shall do the following: (A) Document the oral statement, including, but not limited to, the identity of the law enforcement agency or official making the oral statement and the date upon which the oral statement was made; (B) Limit the delay in reporting the unlawful or unauthorized access to, or use or disclosure of, the patient’s medical information to the date specified in the oral statement, not to exceed 30 calendar days from the date that the oral statement is made, unless a written statement is received during that time. Notice is required no later than five business days after the date designated as the end of the delay.

Permitted delivery of notice:

Not specifically addressed.

WHEN IS NOTICE NOT REQUIRED

Internal paper records, electronic mail, or facsimile transmissions inadvertently misdirected within the same facility or health care system within the course of coordinating care or delivering services shall not constitute unauthorized access to, or use or disclosure of, a patient's medical information.

STATUTE CITATION

Cal. Health and Safety Code § 1280.15

Original bill text:

http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_0301-0350/sb_337_bill_20091011_chaptered.pdf

Amended by S.B. 270:

http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_0251-0300/sb_270_bill_20100929_chaptered.pdf

Statutory code:

<http://www.leginfo.ca.gov/calaw.html>
(Search within the Civil Code / Health and Safety Code for the indicated sections)

ATTORNEY GENERAL

Kamala Harris, Esquire
Attorney General of California
1300 I Street, Suite 1740
Sacramento, CA 95814
916-445-9555

FBI

Los Angeles
11000 Wilshire Blvd.
Suite 1700, FOB
Los Angeles, California 90024-3672
<http://losangeles.fbi.gov>
310-477-6565

Sacramento

4500 Orange Grove Ave.
Sacramento, California 95841-4205
<http://sacramento.fbi.gov>
916-481-9110

San Diego

Federal Office Building
9797 Aero Drive
San Diego, California 92123-1800
<http://sandiego.fbi.gov>
858-565-1255

San Francisco

450 Golden Gate Avenue, 13th. Floor
San Francisco, California 94102-9523
<http://sanfrancisco.fbi.gov>
415-553-7400

SECRET SERVICE

Fresno
559-487-5204

Riverside
951-276-6781

Sacramento

916-325-5481

San Diego

619-557-5640

San Jose

408-535-5288

Santa Ana

714-246-8257

Ventura

805-383-5745

Electronic Crimes Task Force

Los Angeles

213-894-4830

Email: Lax.ectfreports@usss.dhs.gov

Electronic Crimes Task Force

San Francisco

415-744-9026

Email: sfoectf@einformation.usss.gov

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/06

What is a breach:

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information that was, or is reasonably believed to have been acquired by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted, un-redacted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A person that owns or licenses computerized data.
- A person that maintains computerized data must notify and cooperate with the owner or licensee.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay and as soon as possible after a prompt investigation into the likelihood that a security breach will lead to the misuse of personal information.
- Notification may be delayed for legitimate needs of law enforcement if notification would impede a criminal investigation. Law enforcement must make a request to delay notification. Notification is required in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if the person's primary method of communication is electronic or if electronic notice is consistent with E-Sign requirements.
- Telephonic.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 250,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if an investigation determines that misuse of information has not occurred and is not reasonably likely to occur.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are regulated by state or federal law and procedures are maintained pursuant to laws, rules, regulations, or guidelines established by the primary or functional state or federal regulator.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person or a commercial entity maintains its own notification procedures consistent with the timing requirements of state law; and if the person or the commercial entity notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the individual or commercial entity for the purposes of the individual or commercial entity if the personal information is not used for or is not subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of records of publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

ENCRYPTION:

- Notice is not required if the personal information was encrypted.

STATUTE CITATION

Colo. Revised Statutes § 6-1-716

Original bill text:

http://www.state.co.us/gov_dir/leg_dir/olls/sl2006a/sl_145.htm

Statutory code:

<http://www.michie.com/colorado/lpext.dll?f=templates&fn=main-h.htm&cp=>

(Search within the Colorado Revised Statutes for the indicated section)

ATTORNEY GENERAL

John Suthers, Esquire

Attorney General Colorado

1525 Sherman Street

Denver, CO 80203

303-866-4500

FBI

Denver

8000 East 36th Avenue

Denver, Colorado 80238

<http://denver.fbi.gov>

303-629-7171

SECRET SERVICE

Denver

303-850-2700

CONSUMER CREDIT REPORTING

AGENCIES CONTACT

INFORMATION:

Experian®: Send an e-mail to

BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to

businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to

fvad@transunion.com, with “Database Compromise” as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/06

What is a breach:

Unauthorized access to or acquisition of personal information that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Electronic files, media databases or computerized data containing personal information: unencrypted or unsecured by other means that renders personal information unusable or unreadable.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A person that owns or licenses electronic data.
- A person that maintains computerized data must notify the owner or licensee.

Who has to be notified:

- The individual.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- Without unreasonable delay.
- Notification may be delayed for law enforcement if notification would impede a criminal investigation. Law enforcement must make a request to delay notification. Notification is required after the law enforcement agency determines it will not compromise the investigation and so notifies the person to send the notification.
- Notification may be delayed to determine the nature and scope of the breach, identify individuals affected, or to restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if the person's primary method of communication is electronic or if electronic notice is consistent with E-Sign requirements.
- Telephonic.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email (when available); (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER (WITH LIMITATION):

- Notification not required if, after an appropriate investigation and consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that harm will not likely result.

EXISTING POLICY:

- Certain notice requirements may be satisfied if an individual or commercial entity maintains its own security breach procedures consistent with the timing requirements of state law; and notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the individual or commercial entity for the purposes of the individual or commercial entity if the personal information is not used for or is not subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of records of publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

ENCRYPTION:

- Notice is not required if the personal information was encrypted.

STATUTE CITATION

Conn. Statutes § 36a-701b

Original bill text:

<http://www.cga.ct.gov/2005/ACT/Pa/pdf/2005PA-00148-R00SB-00650-PA.pdf>

Statutory code:

<http://www.cga.ct.gov/2009/pub/chap669.htm#Sec36a-701b.htm>

ATTORNEY GENERAL

George Jepsen, Esquire
Attorney General of Connecticut
55 Elm Street
Hartford, CT 06141-0120
860-808-5318

FBI

New Haven
600 State Street
New Haven, Connecticut 06511-6505
<http://newhaven.fbi.gov>
203-777-6311
E-mail: Newhaven@ic.fbi.gov

SECRET SERVICE

New Haven
203-865-2449

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/06

What is a breach:

Unauthorized acquisition or transfer of, or access to, personal health, financial, or personal information, whether or not encrypted, of a Connecticut insured, member, subscriber, policyholder or provider, in whatever form the information is collected, used or stored, which is obtained or maintained by a licensee or registrant of the Insurance Department, the loss of which could compromise or put at risk the personal, financial, or physical well being of the affected insureds, members, subscribers, policyholders or providers.

When is notice required:

- Following an information security incident which affects any Connecticut residents, including breaches by a vendor or business associate of a licensee or registrant.
- Personal health, financial, or personal information, whether or not encrypted, of a Connecticut insured, member, subscriber, policyholder or provider, in whatever form the information is collected, used or stored.
- Personal information: information capable of being associated with a particular individual through one or more identifiers, including, but not limited to (1) Social Security number; (2) a driver's license number; (3) a state identification card number; (4) an account number; (5) a credit or debit card number; (6) a passport number; (7) an alien registration number; or (8) a health insurance identification number.

Who has to notify:

- Licensees and registrants of the Connecticut Insurance Department.

Who has to be notified:

- The Insurance Commissioner.

Required contents of notice:

Notification to the Department should include as much of the following as is known:

- Date of the incident.
- Description of incident (how information was lost, stolen, breached).
- How discovered.
- Has lost, stolen, or breached information been recovered and if so, how.
- Have individuals involved in the incident (both internal and external) been identified.
- Has a police report been filed.
- Type of information lost, stolen, or breached (equipment, paper, electronic, claims, applications, underwriting forms, medical records etc).
- Was information encrypted.
- Lost, stolen or breached information covers what period of time.
- How many Connecticut residents affected.
- Results of any internal review identifying either a lapse in internal procedures or confirmation that all procedures were followed.
- Identification of remedial efforts being undertaken to cure the situation which permitted the information security incident to occur.
- Copies of the licensee/registrants Privacy Policies and Data Breach Policy.
- Regulated entity contact person for the Department to contact regarding the incident. (This should be someone who is both familiar with the details and able to authorize actions for the licensee or registrant).
- Other regulatory or law enforcement agencies notified (who, when).

Draft communications proposed to be made to the affected should also be submitted to the Department.

Timing of notice:

- Notification as soon as a breach is identified, but no later than five calendar days after the breach is identified, to the Insurance Commissioner.

Permitted delivery of notice:

- First class mail.
- Overnight delivery service.
- Email.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if the breach does not pose a potential risk to the privacy of an individual's personal health and/or financial information.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

STATUTE CITATION

Conn. Ins. Dept. Bulletin IC-25

http://www.ct.gov/cid/lib/cid/Bulletin_IC_25_Data_Breach_Notification.pdf

ATTORNEY GENERAL

George Jepsen, Esquire
Attorney General of Connecticut
55 Elm Street
Hartford, CT 06141-0120
860-808-5318

FBI

New Haven
600 State Street
New Haven, Connecticut 06511-6505
<http://newhaven.fbi.gov>
203-777-6311
E-mail: Newhaven@ic.fbi.gov

SECRET SERVICE

New Haven
203-865-2449

SUMMARY OF LAW - EFFECTIVE DATE - 6/28/05

What is a breach:

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account; (4) Individually identifiable information, in electronic or physical form, regarding the Delaware resident's medical history, medical treatment or diagnosis by a health care professional.

Who has to notify:

- A person that owns or licenses computerized data.
- A person that maintains computerized data must notify and cooperate with the owner or licensee.

Who has to be notified:

- The individual.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed for legitimate needs of law enforcement if notification would impede a criminal investigation. Notification is required in good faith without unreasonable delay and as soon as possible after the law enforcement agency determines it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if the person's primary method of communication is electronic or if electronic notice is consistent with E-Sign requirements.
- Telephonic.
- Substitute notice may be done if cost of providing notice exceeds \$75,000 or number of persons exceeds 100,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after a reasonable and prompt investigation is conducted, it is determined that the misuse of information has not and is not reasonably likely to occur.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are regulated by State or federal law and procedures are maintained pursuant to laws, rules, regulations, or guidelines established by the primary or functional State or federal regulator and notice is provided in accordance with these procedures if a breach occurs.

EXISTING POLICY:

- Certain notice requirements may be satisfied if an individual or a commercial entity maintains its own notice procedures consistent with the timing requirements of state law; and if the individual or the commercial entity notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the individual or commercial entity for the purposes of the individual or commercial entity if the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of records of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the personal information was encrypted.

STATUTE CITATION

Del. Code 6 § 12B-101 through 104 (2006)

Original bill text:

[http://legis.delaware.gov/LIS/lis143.nsf/vwLegislation/HB+116/\\$file/legis.html?open](http://legis.delaware.gov/LIS/lis143.nsf/vwLegislation/HB+116/$file/legis.html?open)

Statutory code:

<http://delcode.delaware.gov/title6/c012b/index.shtml>

ATTORNEY GENERAL

Joseph R. Biden, III, Esquire
Attorney General of Delaware
Carvel State Office Building
820 N. French Street
Wilmington, DE 19801
302-577-8338

FBI

Baltimore, MD * *FBI field office Baltimore, MD also covers Delaware*
2600 Lord Baltimore Drive.
Baltimore, MD 21244
<http://baltimore.fbi.gov>
410-265-8080
E-mail: Baltimore@ic.fbi.gov

SECRET SERVICE

Wilmington
302-573-6188

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/07

What is a breach:

Unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

When is notice required:

- Electronic or computerized data containing personal information or equipment storing such data that has not been rendered secure so as to be unusable by an unauthorized third party.
- Personal information: (I) First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) credit card number or debit card number; OR (II) any other number or code or combination, such as account number, security code, access code, or password, that allows access to an individual's financial or credit account.

Who has to notify:

- A person that owns or licenses electronic or computerized data.
- A person that maintains computerized data must notify the owner or licensee.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed for law enforcement if notification would impede a criminal investigation. Notification is required as soon as possible after the law enforcement agency determines it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if the consumer consents or if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$50,000 or number of persons exceeds 100,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major local, and if applicable, national media.

WHEN IS NOTICE NOT REQUIRED

STATUTORY:

- Notice is not required to credit reporting agencies under the statute if the entity is subject to the Gramm-Leach-Bliley Act (GLB).

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person or business maintains its own notification procedures consistent with the timing requirements of state law; and if the person or business provides notice, in accordance with its policies, reasonably calculated to give actual notice to affected individuals.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business if the personal information is not used improperly or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the data has been rendered secure, so as to be unusable by an unauthorized third party.

STATUTE CITATION

D.C. Code § 28-3851 through 53

Original bill text:

<http://www.dccouncil.washington.dc.us/images/00001/20061218135855.pdf>

Statutory code:

<http://government.westlaw.com/linkedslice/default.asp?SP=DCC-1000>
(See Division 5, Title 28, Subtitle II, Chapter 38, Subchapter II for the indicated sections)

ATTORNEY GENERAL

Irvin Nathan, Esquire
Attorney General of the
District of Columbia
John A. Wilson Building
1350 PA Avenue, NW, Suite 409
Washington, DC 20009
202-727-3400

FBI

Washington
Washington Metropolitan Field Office
601 4th Street, N.W.
Washington, D.C. 20535-0002
<http://washingtondc.fbi.gov>
202-278-2000
E-mail: Washington.field@ic.fbi.gov

SECRET SERVICE

Washington DC
202-406-8000

Electronic Crimes Task Force
Washington DC
202-406-8500

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to
BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to
businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to
fvad@transunion.com, with "Database
Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/05

What is a breach:

Unlawful and unauthorized acquisition of unencrypted data that compromises the security, confidentiality, or integrity of personal information that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Personal information: First name or first initial and last name or any middle name and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A person with a direct business relationship with the resident or pursuant to an agreement.
- A person that maintains computerized data must notify the owner or licensee within 10 business days.

Who has to be notified:

- The individual.
- The business entity on whose behalf data is maintained.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice in a single occurrence.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- Without unreasonable delay, but no later than 45 days following determination of the breach or notice from law enforcement.
- Notification may be delayed for legitimate needs of law enforcement if notification would impede a criminal investigation. Notification is required after the law enforcement agency determines it will not compromise the investigation.
- Notification may be delayed to determine the presence, nature and scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if consumer consent and consistent with E-Sign OR if the person or business providing the notice has a valid e-mail address for the subject person and the subject person has agreed to accept communications electronically.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after an appropriate investigation or after consultation with relevant law enforcement, it is determined that the breach has not and will not likely result in harm.
- The determination must be documented in writing for five years.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are subject to rules, regulations, procedures or guidelines established by their federal functional regulator, if notice is made in accordance with those requirements in the event of a breach.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person or business maintains its own notification procedures consistent with the timing requirements of state law; and if the person or business provides notice, in accordance with its policies, reasonably calculated to give actual notice to affected individuals.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business if the personal information is not used improperly or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the data has been rendered secure, so as to be unusable by an unauthorized third party.

STATUTE CITATION

Fla. Statutes Ann. title 46 § 817.5681
[Original bill text:
 http://www.flsenate.gov/data/
 session/2005/House/bills/billtext/pdf/
 h048105er.pdf](http://www.flsenate.gov/data/session/2005/House/bills/billtext/pdf/h048105er.pdf)

Statutory code:
[http://www.leg.state.fl.us/statutes/
 index.cfm?mode=View%20
 Statutes&SubMenu=1&App_
 mode=Display_Statute&Search_Strin
 g=817.5681&URL=0800-0899/0817/
 Sections/0817.5681.html](http://www.leg.state.fl.us/statutes/index.cfm?mode=View%20Statutes&SubMenu=1&App_mode=Display_Statute&Search_Strin_g=817.5681&URL=0800-0899/0817/Sections/0817.5681.html)

ATTORNEY GENERAL

Pam Bondi, Esquire
 Attorney General of Florida
 The Capitol
 PL 01
 Tallahassee, FL 32399-1050
 850-414-3300

FBI

Jacksonville
 6061 Gate Parkway
 Jacksonville, Florida 32256
<http://jacksonville.fbi.gov>
 904-248-7000

North Miami Beach

16320 Northwest Second Avenue
 North Miami Beach, Florida 33169-6508
<http://miami.fbi.gov>
 305-944-9101

Tampa

5525 West Gray Street
 Tampa, Florida 33609
<http://tampa.fbi.gov>
 813-253-1000

SECRET SERVICE

Fort Myers
 239-334-0660

Jacksonville
 904-296-0133

Miami
 305-863-5000

Tallahassee
 850-942-9523

Tampa
 813-228-2636

West Palm Beach
 561-659-0184

Electronic Crimes Task Force
 Miami

305-863-5450

Email: miaectf@einformation.usss.gov
 Electronic Crimes Task Force

Orlando

407-648-6333

Email: orlecgw@einformation.usss.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to
[BusinessRecordsVictimAssistance@
 Experian.com](mailto:BusinessRecordsVictimAssistance@Experian.com).

Equifax®: Send an e-mail to
businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to
fvad@transunion.com, with "Database
 Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 5/5/05

What is a breach:

Unauthorized acquisition of unencrypted data that compromises the security, confidentiality, or integrity of personal information that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Electronic or computerized data containing personal information: unencrypted or unredacted.
- Personal information: First name or first initial or middle name and last name in combination with (1) Social Security number; (2) drivers license or identification card number; (3) account number, credit card number or debit card number if such a number could be used without additional identifying information, access codes, or passwords; (4) account passwords or personal identification numbers or other access codes; or (5) any of the items listed in 1-4 when not in connection with the individual's first name or first initial and last name if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

Who has to notify:

- An information broker.
- A person that maintains computerized data on behalf of an information broker must notify the information broker within 24 hours following discovery of the breach.

Who has to be notified:

- The individual.
- The information broker on whose behalf the data is maintained.
- The nationwide credit reporting agencies must be notified if more than 10,000 individuals receive notice at one time.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed for legitimate needs of law enforcement if notification would compromise a criminal investigation. Notification is required after the law enforcement agency determines it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system.

Permitted delivery of notice:

- Written.
- Telephonic.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$50,000 or number of persons exceeds 100,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

EXISTING POLICY:

- Certain notice requirements may be satisfied if an information broker or data collector maintains its own notification procedures consistent with the timing requirements of state law; and if it notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition or use of personal information by an employee or agent of an information broker or data collector for the purposes of such information broker or data collector provided that the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the data has been encrypted so as to be unusable by an unauthorized third party, and has not, or is not reasonably believed to have been, acquired by an unauthorized person.

STATUTE CITATION

Ga. Code 10 § 10-1-912 (2006)

Original bill text:

http://www.legis.state.ga.us/legis/2005_06/fulltext/sb230.htm

Statutory code:

<http://www.lexis-nexis.com/hottopics/gacode/> (Copyright protected – search for the indicated section)

ATTORNEY GENERAL

Sam Olens, Esquire
Attorney General Georgia
40 Capitol Square, SW
Atlanta, GA 30334-1300
404-656-3300

FBI

Atlanta
2635 Century Parkway, Northeast
Suite 400
Atlanta, Georgia 30345-3112
<http://atlanta.fbi.gov>
404-679-9000

SECRET SERVICE

Albany
229-430-8442

Savannah
912-652-4401

Electronic Crimes Task Force

Atlanta
404-331-6111
Email: Atlantaectf@ussd.dhs.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with “Database Compromise” as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/07

What is a breach:

(I) Unauthorized access to and acquisition of unencrypted or un-redacted records or data where the illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person; OR (II) or unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key.

When is notice required:

- Records or data containing personal information: unencrypted or encrypted with the confidential process or key.
- Personal information: First name or first initial or middle name and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) account number, credit card number or debit card number, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A person that owns or licenses information.
- A person that maintains computerized data must notify the owner or licensee.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- The State's Office of Consumer Protection must be notified without unreasonable delay if more than 1,000 individuals receive notice at a single time.

Required contents of notice:

- The incident.
- The type of personal information subjected to unauthorized access and acquisition.
- The general acts of the business to protect the personal information.
- A telephone number the person may call for further information and assistance, if available.
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Timing of notice:

- Without unreasonable delay.
- Notification may be delayed for legitimate needs of law enforcement if notification would impede a criminal investigation or jeopardize national security. Request may be made by law enforcement in writing or the business should document contemporaneously the request along with a name of the officer and requesting agency. Notification is required after the law enforcement agency communicates its determination that it will not compromise the investigation or jeopardize national security.
- Notification may be delayed to determine sufficient contact information, the scope of the breach, and restore the reasonable integrity, security and confidentiality of the system.

Permitted delivery of notice:

- Written to the last available address the business has on record.
- Electronic, if the business has a valid email address, consumer consent, and the email is consistent with E-Sign requirements.
- Telephonic, provided that contact is made directly with the affected person.
- Substitute notice may be done if cost of providing notice exceeds \$100,000 or number of persons exceeds 200,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if illegal use of the personal information has not occurred, is not reasonably likely to occur, or does not create a risk of harm.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.
- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are health care plans or health care providers subject to and in compliance with the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition or use of personal information by an employee or agent of business for a legitimate purpose provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the personal information has been encrypted or encrypted records or data containing personal information has not been acquired along with the confidential process or key.

STATUTE CITATION

HRS § 487N-1 through § 487N-4

Original bill text:

http://www.capitol.hawaii.gov/session2006/Bills/SB2290_CD1_.pdf

Statutory code:

http://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487N/HRS_0487N-0001.htm

(Use the navigation keys at the bottom of the screen to access the additional indicated sections)

ATTORNEY GENERAL

David Louie, Esquire
Attorney General of Hawaii
425 Queen Street
Honolulu, HI 96813
808-586-1500

FBI

Honolulu
Prince Kuhio FOB
300 Ala Moana Boulevard
Suite 4-230
Honolulu, Hawaii 96813
<http://honolulu.fbi.gov>
808-566-4300

SECRET SERVICE

Honolulu
808-541-1912

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with “Database Compromise” as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/06

What is a breach:

Illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality or integrity of personal information.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A person that owns or licenses computerized data.
- A person that maintains computerized data must notify and cooperate with the owner or licensee.

Who has to be notified:

- The individual.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- In good faith and without unreasonable delay and in the most expedient time possible.
- Notification may be delayed until after a law enforcement agency advises that it will no longer impede a criminal investigation.
- Notification may be delayed to determine the scope of the breach, identify individuals affected, and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written to the most recent address in the entity's records.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Telephonic.
- Substitute notice may be done if cost of providing notice exceeds \$25,000 or number of persons exceeds 50,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after an investigation is conducted, it is determined there is no likelihood that personal information has been or will be misused.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are regulated by state or federal law and procedures are maintained pursuant to laws, rules, regulations, or guidelines established by the primary or functional state or federal regulator and if notice complies with the maintained procedures.

EXISTING POLICY:

- Certain notice requirements may be satisfied if an individual or a commercial entity maintains its own notice procedures consistent with the timing requirements of state law, and notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity provided that the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

ENCRYPTION:

- Notice is not required if the data has been encrypted and does not materially compromise the security, confidentiality, or integrity of personal information.

STATUTE CITATION

Idaho Code title 28 § 51-105

Original bill text

<http://legislature.idaho.gov/legislation/2006/S1374.html#>

Statutory code:

<http://legislature.idaho.gov/idstat/Title28/T28CH51SECT28-51-104.htm>;

<http://www.legislature.idaho.gov/idstat/Title28/T28CH51SECT28-51-105.htm>

ATTORNEY GENERAL

Lawrence Wasden, Esquire

Attorney of General Idaho

700 W. Jefferson Street

P.O Box 83720

Boise, ID 83720

208-334-2424

FBI

Salt Lake City, UT * *FBI field office Salt Lake City, UT also covers surrounding areas*

257 East 200 South

Suite 1200

Salt Lake City, UT 84111-2048

801-579-1400

<http://saltlakecity.fbi.gov>

E-mail: SaltLakeCity@ic.fbi.gov

SECRET SERVICE

Boise

208-334-1403

SUMMARY OF LAW - EFFECTIVE DATE - 6/27/06; AMENDMENTS EFFECTIVE 1/1/12

What is a breach:

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information.

When is notice required:

- Computerized data containing personal information: unencrypted or unredacted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- Any data collector.
- A person that maintains or stores, but does not own or license, computerized data must notify the owner or licensee. In addition to requiring notice to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach including but not limited to: (1) Informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (2) Informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach.

Who has to be notified:

- An Illinois resident at no charge.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

- The toll-free numbers and addresses for consumer reporting agencies.
- The toll-free number, address, and website address for the Federal Trade Commission, and
- A statement that the individual can obtain information from these sources about fraud alerts and security freezes.
- The notification shall not include information concerning the number of Illinois residents affected by the breach.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if an appropriate law enforcement agency requests the delay in writing based on a determination that notification will interfere with a criminal investigation. Notice is required as soon as it will no longer interfere with the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

EXISTING POLICY:

- Certain notice requirements may be satisfied if a data collector maintains its own notification procedures consistent with the timing requirements of state law; and notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for an unrelated purpose or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

STATUTE CITATION

Ill. Statutes 815 § 530-10

Original bill text:

<http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=094-0036&GA=094>

Amended by HB 3025:

<http://www.ilga.gov/legislation/publicacts/97/PDF/097-0483.pdf>

Statutory code:

<http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67>

ATTORNEY GENERAL

Lisa Madigan, Esquire
Attorney General of Illinois
James R. Thompson Center
100 W. Randolph Street
Chicago, IL 60601
312-814-3000

FBI

Chicago
2111 West Roosevelt Road
Chicago, IL 60608-1128
<http://chicago.fbi.gov>
312-421-6700
E-mail: Chicago@ic.fbi.gov

Springfield
900 East Linton Avenue
Springfield, Illinois 62703
<http://springfield.fbi.gov>
217-522-9675
E-mail: Springfield@ic.fbi.gov

SECRET SERVICE

Springfield
217-726-8453

Electronic Crimes Task Force
Chicago
312-353-5431
Fax: 312-353-1225

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/06; AMENDMENTS EFFECTIVE 7/1/09

What is a breach:

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person.

- The term includes the unauthorized acquisition of computerized data that has been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.
- The term does not include unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key: (1) has not been compromised or disclosed; and (2) is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device.

When is notice required:

- Computerized data containing personal information: unencrypted or unredacted.
- Personal information: A Social Security number that is not encrypted, OR first name or first initial and last name in combination with (1) drivers license, (2) identification card number; or (3) credit card number; or (4) account number or debit card number in combination with a required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A person that owns or licenses computerized data.
- A person that maintains computerized data must notify the owner or licensee.

Who has to be notified:

- The individual.
- State Attorney General.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- Without unreasonable delay.
- Notification may be delayed if in response to a request from the attorney general or a law enforcement agency because it will impede a criminal or civil investigation or jeopardize national security. Notification is required as soon as possible after the attorney general or the law enforcement agency notifies that delay will no longer impede the investigation or jeopardize national security.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if an email address is available.
- Telephonic.
- Facsimile.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) web site posting and (iii) notice to major news reporting media in the geographic area of the affected residents.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER

- Notice is not required if the breach has not resulted in or could result in identity deception, identity theft, or fraud.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are an information privacy, security policy, or compliance plan is maintained and in compliance under:

- Patriot Act (P.L. 107-56);
- Executive Order 13224;
- Driver's Privacy Protection Act (18 U.S.C. 2781 et seq.);
- Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
- Gramm-Leach-Bliley Act (GLB) Act (15 U.S.C. 6801 et seq.); or
- Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191);

and the entity's policy requires notice without unreasonable delay and the entity complies with that policy. The plan must also maintain reasonable procedures to protect and safeguard personal information from unlawful use or disclosure.

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are subject to Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a data base owner maintains its own disclosure procedures for affected individuals to be notified of a breach without unreasonable delay and the data base owner complies with the plan.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if unencrypted personal information was not acquired by an unauthorized person; or encrypted personal information was not acquired by an unauthorized person with access to the encryption key.

STATUTE CITATION

Ind. Code § 24-4.9

Original bill text:

<http://www.in.gov/legislative/bills/2006/PDF/HE/HE1101.1.pdf>

Amendment text: <http://www.in.gov/legislative/bills/2009/PDF/HE/HE1121.1.pdf>

<http://www.in.gov/legislative/bills/2009/PDF/HE/HE1121.1.pdf>

Statutory code:

<http://www.in.gov/legislative/ic/code/title24/ar4.9/>

ATTORNEY GENERAL

Greg Zoeller, Esquire

Attorney General of Indiana
Indiana Government Center South
5th Floor
302 West Washington Street
Indianapolis, IN 46204
317-232-6201

FBI

Indianapolis

8825 Nelson B Klein Pkwy
Indianapolis, Indiana 46204
<http://indianapolis.fbi.gov>
317-595-4000

E-mail: Indianapolis@ic.fbi.gov

SECRET SERVICE

Indianapolis
317-635-6420

CONSUMER CREDIT REPORTING

AGENCIES CONTACT

INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/08

What is a breach:

Unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information maintained by the person.

When is notice required:

- Computerized data containing personal information: unencrypted, unredacted, or otherwise unaltered by any method or technology in such a manner that the name or computerized data containing personal information is unreadable.
- Personal information: (1) Social Security number; (2) drivers license or other unique identification number created or collected by a government body; (3) financial account number, credit card or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; (4) unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (5) unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

Who has to notify:

- A person that maintains the information.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

- Notice at a minimum will include all of the following:
- A description of the breach of security.
- The approximate date of the breach of security.
- The type of personal information obtained as a result of the breach of security.
- Contact information for consumer reporting agencies.
- Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.

Timing of notice:

- The most expeditious manner possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. Notification is required after the law enforcement agency determines that it will not compromise the investigation and notifies the person required to give notice in writing.
- Notification may be delayed to determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.

Permitted delivery of notice:

- Written to the last available address in person's records.
- Electronic, if the person's customary method of communication with the consumer is by electronic means or if consistent with E-Sign.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 350,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, it is determined that there is no reasonable likelihood of financial harm.
- The determination must be documented in writing for five years.

STATUTORY:

- Certain state provisions do not apply if the entity is in compliance with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements than that provided by state law.
- Certain state provisions do not apply if the entity is subject to and in compliance with regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act (GLB).
- Certain state provisions do not apply if the entity is in compliance with notification procedures that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by this state law pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

PUBLIC RECORDS:

- Notice is not required if the information consists of personal information that may be lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public.

STATUTE CITATION

Iowa Code § 715C.1 through § 715C.2

Original bill text:

<http://coolice.legis.state.ia.us/Cool-ICE/default.asp?Category=BillInfo&Service=Billbook&ga=82&hbill=SF2308>

Statutory code:

<http://coolice.legis.state.ia.us/Cool-ICE/default.asp?category=billinfo&service=iowaCode&ga=83&input=715C.1;>

<http://coolice.legis.state.ia.us/Cool-ICE/default.asp?category=billinfo&service=iowaCode&ga=83&input=715C.2>

ATTORNEY GENERAL

Tom Miller, Esquire
Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut
Des Moines, IA 50319
515-281-5164

FBI

Omaha, NE * *FBI field office Omaha, NE also covers Iowa*
4411 South 121st Court
Omaha, Nebraska 68137-2112
<http://omaha.fbi.gov>
402-493-8688
E-mail: Omaha@ic.fbi.gov

Omaha Mailing Address * *FBI field office Omaha, NE also covers Iowa*
4411 South 121st Court
Omaha, Nebraska 68137-2112

SECRET SERVICE

Des Moines
515-284-4565

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/06

What is a breach:

Unauthorized access and acquisition of unencrypted computerized data that materially compromises the security, confidentiality or integrity of personal information and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft.

When is notice required:

- Computerized data containing personal information: unencrypted, unredacted, or otherwise unaltered by any method or technology in such a manner that the name or personal information is unreadable.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) financial account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A person that maintains computerized data must notify the owner or licensee.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that notice will impede a criminal investigation. Notification is required without unreasonable delay, as soon as possible after the law enforcement agency determines it will no longer impede the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$100,000 or number of persons exceeds 5,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if an investigation determines there is no reasonable likelihood that personal information has been or will be misused.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they maintain breach procedures pursuant to laws, rules, regulations, or guidelines established by the primary or functional state or federal regulator.

EXISTING POLICY:

- Certain notice requirements may be satisfied if an individual or a commercial entity maintains its own notification procedures consistent with the timing requirements of state law; and notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity provided that the personal information is not used for or is not subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state or local government records.

ENCRYPTION:

- Notice is not required if personal information is encrypted or redacted.

STATUTE CITATION

K.S.A. § 50-7a01 through 50-7a02

Original bill text:

<http://www.kslegislature.org/bills/2006/3003.pdf>

Statutory code:

http://kslegislature.org/li/m/statute/050_000_0000_chapter/050_007a_0000_article/index.html

ATTORNEY GENERAL

Derek Schmidt, Esquire
Attorney General of Kansas
120 S.W. 10th Avenue, 2nd Floor
Topeka, KS 66612-1597
785-296-2215

FBI

Kansas City, MO
1300 Summit St.
Kansas City, Missouri 64105-1362
<http://kansascity.fbi.gov>
816-512-8200
E-mail: Kansas.city@ic.fbi.gov

SECRET SERVICE

Wichita
316-267-1452

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/06

What is a breach:

Compromise of the security, confidentiality or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information.

When is notice required:

- Computerized data containing personal information: unencrypted or unredacted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A data owner or licensee.
- A person that maintains computerized data must notify the owner or licensee.

Who has to be notified:

- The individual.
- The Consumer Protection Section of the Attorney General's Office. Notice shall be written and include the names of all Louisiana citizens affected by the breach.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after a law enforcement agency determination that it will no longer compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.
- Notice to the attorney general shall be timely if received within 10 days of distribution of notice to Louisiana citizens. Each day notice is not received by the attorney general shall be deemed a separate violation. Failure to provide timely notice may be punishable by a fine not to exceed \$5,000 per violation.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

Regulatory Authority:

- The provisions of this Chapter shall not take effect until rules are promulgated by the attorney general's office.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after investigation, it is determined that there is no reasonable likelihood of harm.

STATUTORY:

- Financial Institutions are deemed to be in compliance with some or all of the state statute's requirements if they are subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person maintains a notification procedure consistent with the timing requirements of state law; and notifies affected individuals in accordance with its policy and procedure.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of a person for the purposes of the person, provided that the personal information is not used for, or is subject to, unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state or local government records.

ENCRYPTION:

- Notice is not required if personal information is encrypted or redacted.

STATUTE CITATION

La. Rev. Stat. 51 § 3071 through 3077

Original bill text:

<http://www.legis.state.la.us/billdata/streamdocument.asp?did=320093>

Statutory code:

<http://www.legis.state.la.us/lss/lss.asp?doc=322030> (Use the navigation keys at the top of the screen to access the additional indicated sections)

Louisiana Administrative Code Title 16,
Section 701

<http://doa.louisiana.gov/osr/lac/16v01/16v01.doc>

ATTORNEY GENERAL

James D. Caldwell, Esquire

Attorney General of Louisiana

P.O. Box 94005

Baton Rouge, LA 70804

225-326-6079

Attention: Consumer Protection Division

P.O. Box 94005

Baton Rouge, LA 70802

225-326-6465

FBI

FBI New Orleans

2901 Leon C. Simon Blvd.

New Orleans, Louisiana 70126

<http://neworleans.fbi.gov>

504-816-3000

SECRET SERVICE

Baton Rouge

225-925-5436

New Orleans

504-841-3260

SUMMARY OF LAW - EFFECTIVE DATE - 1/31/06; AMENDMENTS EFFECTIVE 9/11/09

What is a breach:

The unauthorized acquisition, release or use of an individual's computerized data that includes personal information that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person.

When is notice required:

- Computerized data containing personal information: unencrypted or unredacted.
- Personal information: First name or first initial and middle name and last name in combination with (1) Social Security number; (2) drivers license or identification card number; (3) account number, credit card number or debit card number if such a number could be used without additional identifying information, access codes, or passwords; (4) account passwords or personal identification numbers or other access codes; or (5) any of the items listed in 1-4 when not in connection with the individual's first name or first initial and last name if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

Who has to notify:

- A person that maintains computerized data.
- A third party that maintains computerized data on behalf of a person must notify the person.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- The appropriate state regulators within the Department of Professional and Financial Regulation, or if not regulated by this Department, the Attorney General.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- As expediently as possible and without unreasonable delay.
- Notification may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$5,000 or number of persons exceeds 1,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

Regulatory Authority:

- With respect to persons under the jurisdiction of the regulatory agencies of the Department of Professional and Financial Regulation, the appropriate state regulators within that department may adopt rules as necessary for the administration and implementation of these requirements. With respect to all other persons, the Attorney General may adopt rules as necessary for the administration and implementation of these requirements.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after a reasonable and prompt investigation, it is determined that personal information has not been or will not be misused or if it is not reasonably possible that misuse will occur.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition release of use of personal information by an employee or agent of a person on behalf of the person if the personal information is not used for or subject to further unauthorized disclosure to another person.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

STATUTE CITATION

10 M.R.S. § 1348

Original bill text:

http://www.mainelegislature.org/legis/bills/bills_122nd/billtexts/LD167101-1.asp (Use the navigation keys at the top of the screen to access additional text of the bill)

Amendment text: http://www.mainelegislature.org/legis/bills/bills_124th/chapters/PUBLIC161.asp

Statutory code:

<http://janus.state.me.us/legis/statutes/10/title10sec1348.html>

Statutory Code:

<http://www.mainelegislature.org/legis/statutes/10/title10sec1348.pdf>

ATTORNEY GENERAL

William Schneider, Esquire
Attorney General of Maine
State House Station 6
Augusta, ME 04333
207-626-8800

Linda Conti, Esquire
Assistant Attorney General
Consumer Protection Division
State House Station 6
Augusta, ME 04333
207-626-8591

FBI

Boston, MA * *FBI field Office Boston, MA also covers Maine*
One Center Plaza
Suite 600
Boston, Massachusetts 02108
<http://boston.fbi.gov>
617-742-5533
E-mail: Boston@ic.fbi.gov

SECRET SERVICE

Portland
207-780-3493

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/08

What is a breach:

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business.

When is notice required:

- Computerized data containing personal information: unencrypted, redacted, or otherwise unprotected by another method that renders the data unreadable or unusable.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number; (3) financial account number, including a credit card number or debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account; or; (4) individual taxpayer identification number.

Who has to notify:

- A business or state entity that owns or licenses records that includes personal information of an individual residing in the state.
- A person that maintains computerized data must notify the owner or licensee.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- The Office of the Attorney General prior to giving the required notification.

Required contents of notice:

- A description of the information categories acquired, including which elements of personal information.
- Contact info for the business making the notification (address, telephone number, and toll-free telephone number if maintained).
- Toll-free telephone numbers and addresses for the major consumer reporting agencies.
- Toll-free telephone numbers, addresses, and website addresses for: (1) Federal Trade Commission, (2) Attorney General Office, and (3) a statement that an individual can obtain information from these sources on steps to avoid identity theft.

Timing of notice:

- As soon as reasonably practicable.
- Notification may be delayed if notification will impede a criminal investigation or jeopardize homeland or national security. Notification is required as soon as reasonably practicable after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security.
- Notification may be delayed to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system.

Permitted delivery of notice:

- Written to the most recent address in the business' records.
- Electronic, if the individual has expressly consented to receive electronic notice and if the business conducts its business primarily through Internet account transactions or the Internet.
- Telephonic to the most recent telephone number in the business' records.
- Substitute notice may be done if cost of providing notice exceeds \$100,000 or number of persons exceeds 175,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after conducting in good faith a reasonable and prompt investigation, it is determined that misuse of personal information has not occurred or is not reasonably likely to occur.
- The determination must be maintained in records for three years.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are in compliance with the requirements for notification procedures under the rules, regulations, procedures, or guidelines established by the primary or functional federal or state regulator.
- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are subject to and in compliance with the Gramm-Leach-Bliley Act (GLB) Safeguards Rule, the Fair Credit Reporting Act Disposal Rule, and the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Affiliates of businesses also can be covered by this provision if they comply with the foregoing.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of a business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.
- Notice is not required if the information is Information that an individual has consented to have publicly disseminated or listed.

ENCRYPTION:

- Notice is not required if the personal information is encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable.

HEALTH INFORMATION:

- Notice is not required if the information subject to the breach is disseminated or listed in accordance with Health Insurance Portability and Accountability Act (HIPAA).

STATUTE CITATION

Md. Commercial Law Code Ann. § 14-3501 through 08

Original bill text:

http://mlis.state.md.us/2007RS/chapters_noIn/Ch_532_hb0208E.pdf

Statutory code:

<http://www.lexisnexis.com/hottopics/mdcode/> (See Maryland Code, Commercial Law, Title 14, Subtitle 35 for the indicated sections)

ATTORNEY GENERAL

Douglas F. Gansler, Esquire
Attorney General of Maryland
200 St. Paul Place
Baltimore, MD 21202-2202
410-576-6300

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
410-576-6491
ldtheft@oag.state.md.us

FBI

Baltimore
2600 Lord Baltimore Drive
Baltimore, Maryland 21244
<http://baltimore.fbi.gov>
410-265-8080
E-mail: Baltimore@ic.fbi.gov

SECRET SERVICE

Electronic Crimes Task Force
Baltimore
443-263-1000
Fax: 443-263-1100
Email: balecwg@einformation.usss.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with “Database Compromise” as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 10/31/07

What is a breach:

The unauthorized acquisition or unauthorized use of unencrypted data, or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident.

When is notice required:

- Computerized data containing personal information: unencrypted or encrypted with the confidential process or key.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) financial account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A data owner or licensee.
- A person that maintains computerized data must notify and cooperate with the owner or licensee.

Who has to be notified:

- The individual.
- The Attorney General and Director of Consumer Affairs and Business Regulation.
- Any relevant consumer reporting agency or state agency, as deemed appropriate and identified and forwarded by the Director of Consumer Affairs and Business Regulation.

Required contents of notice:

Shall include:

- Individual's right to obtain a police report.
- How to request a security freeze and necessary information to be provided when requesting a security freeze and any fees.
- Notification shall not include the nature of the breach or the number of residents affected by the breach.

Timing of notice:

- As soon as practicable and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it will no longer pose a risk to the investigation and so informs the Attorney General in writing and the person required to send notification.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) publication/broadcast through media that provides notice throughout the Commonwealth.

Regulatory Authority:

- The department of consumer affairs and business regulation may adopt regulations, from time to time, to revise the definition of "encrypted" to reflect applicable technological advancements.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if the unauthorized acquisition or unauthorized use of covered data does not create a substantial risk of identity theft or fraud.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they maintain procedures pursuant to federal laws, rules, regulations, guidance, or guidelines, if notice is in accordance with the maintained or required procedures when a breach occurs; provided further that the attorney general and the director of the office of consumer affairs and business regulation of the breach is notified as soon as practicable and without unreasonable delay.

GOOD FAITH:

- Notice is not required if there has been a good faith but unauthorized acquisition of personal information by a person, or employee or agent thereof, for the lawful purposes of such person, unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of information lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

ENCRYPTION:

- Notice is not required if the personal information is encrypted data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information has not been compromised.

STATUTE CITATION

ALM GL CHAPTER 93H

[Original bill text:](#)

[Not available.](#)

[Statutory code: http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h](http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h)

ATTORNEY GENERAL

Martha Coakley, Esquire
Attorney General of Massachusetts
1 Ashburton Place
Boston, MA 02108-1518
617-727-2200

Office of Consumer Affairs & Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116
Phone: (617) 973-8700

FBI

Boston
One Center Plaza
Suite 600
Boston, Massachusetts 02108
<http://boston.fbi.gov>
617-742-5533
E-mail: Boston@ic.fbi.gov

SECRET SERVICE

Electronic Crimes Task Force
Boston
617-565-5640
Email: bosectf@einformation.usss.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 7/2/07

What is a breach:

The unauthorized access and acquisition of data that compromises the security, confidentiality, or integrity of personal information.

When is notice required:

- Unencrypted and unredacted personal information.
- Encrypted personal information accessed or acquired with the encryption key.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; (3) demand deposit or other financial account number, or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to any resident's financial account.

Who has to notify:

- A data owner or licensee.
- A person pursuant to an agreement with the data owner or licensee.
- A person that maintains data must notify the owner or licensee.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

The breach notification shall be clear and conspicuous:

- Describe the security breach in general terms.
- Describe the type of personal information that is the subject of the unauthorized access or use.
- Describe what the agency or person providing notice has done to protect data from further security breaches.
- Include a telephone number where a notice recipient may obtain assistance or additional information.
- Remind notice recipients of the need to remain vigilant for incidents of identity theft and fraud.

Timing of notice:

- Without unreasonable delay.
- Notification may be delayed if a law enforcement agency advises the person that it will impede a criminal or civil investigation or jeopardize homeland or national security. Notification is required after the law enforcement agency determines that it will no longer impede the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written to the postal address in the person's records.
- Electronic if (1) consumer express consent to receive electronic notice and (2) the existing business relationship includes periodic e-mails so that the person reasonably believes that it has the recipient's current e-mail address and (3) the person conducts its business primarily through internet account transactions or on the internet.
- Telephonic, if the notice is not given by use of a recorded message; or if there is express consumer consent to receive telephone notice; or if there is no express consent but the person also provides written and email notice and if a live conversation results within 3 business days after the initial attempt.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if it is determined that the security breach has not or is not likely to cause substantial loss or injury, or result in identity theft.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are subject to, and notification procedures are in place that are in compliance with, the interagency guidance on response programs for unauthorized access to customer information and customer notice or similar guidance prescribed and adopted by the national credit union administration, and its affiliates.
- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are subject to and in compliance with Health Insurance Portability and Accountability Act (HIPAA).
- Notice to credit reporting agencies is not required under state statute by persons subject to Title V of the Gramm-Leach-Bliley Act (GLB).

GOOD FAITH:

- Notice is not required if the access by an employee or other individual meets all of the following:
 - (i) The employee or other individual acted in good faith in accessing the data.
 - (ii) The access was related to the activities of the person.
 - (iii) The employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person.

PUBLIC RECORDS:

- Notice is not required if the information consists of federal, state, or local government records or documents lawfully made available to the general public.

ENCRYPTION:

- Notice is not required if the personal information was encrypted or redacted unless the personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.

STATUTE CITATION

MCL § 445.61 and MCL § 445.72

Original bill text:

<http://www.legislature.mi.gov/documents/2005-2006/publicact/pdf/2006-PA-0566.pdf>

Statutory code:

[http://www.legislature.mi.gov/\(S\(prtuyd45133ci055xwtmj045\)\)/mileg.aspx?page=getObject&objectName=mcl-445-63&highlight=445.61;](http://www.legislature.mi.gov/(S(prtuyd45133ci055xwtmj045))/mileg.aspx?page=getObject&objectName=mcl-445-63&highlight=445.61;)

[http://www.legislature.mi.gov/\(S\(npd3i3jqn1smw45o3ocw545\)\)/mileg.aspx?page=GetObject&objectName=mcl-445-72](http://www.legislature.mi.gov/(S(npd3i3jqn1smw45o3ocw545))/mileg.aspx?page=GetObject&objectName=mcl-445-72)

ATTORNEY GENERAL

Bill Schuette, Esquire
Attorney General of Michigan
525 W. Ottawa Street
P.O. Box 30212
Lansing, MI 48909-0212
517-373-1110

FBI

Detroit
P. V. McNamara FOB
477 Michigan Avenue
26th Floor
Detroit, Michigan 48226
<http://detroit.fbi.gov>
313-965-2323

SECRET SERVICE

Detroit
313-226-6400
Grand Rapids
616-454-4671
Saginaw
989-497-0580

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with “Database Compromise” as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/06

What is a breach:

The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to any resident's financial account.

Who has to notify:

- A data owner or licensee.
- A person that maintains the data must notify the owner or licensee.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified within 48 hours if more than 500 individuals receive notice at one time.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed to a date certain if a law enforcement agency determines that it will impede a criminal investigation. Notification is required afterward.
- Notification may be delayed to determine the scope of the breach, to identify the individuals affected, and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written to the most recent address in the person's/business' records.
- Electronic, if the person's primary method of communication is electronic or if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

STATUTORY:

- Some or all state provisions do not apply to the Gramm-Leach-Bliley Act (GLB) financial institutions.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person or business maintains its own notification procedures consistent with the timing requirements of state law; and if the person or business notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business, provided that the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the personal information is encrypted.

STATUTE CITATION

Minn. Statutes § 325E.61

Original bill text:

<http://www.revisor.leg.state.mn.us/bin/bldbill.php?bill=H2121.3&session=1s84>

Statutory code:

<https://www.revisor.mn.gov/statutes/?id=325E.61>

ATTORNEY GENERAL

Lori Swanson, Esquire
Attorney General of Minnesota
State Capitol, Suite 102
1400 Bremer Tower
445 Minnesota Street
St. Paul, MN 55155-2131
651-296-3353

FBI

Minneapolis
111 Washington Avenue South
Suite 1100
Minneapolis, Minnesota 55401-2176
<http://minneapolis.fbi.gov>
612-376-3200

SECRET SERVICE

Electronic Crimes Task Force
Minneapolis
612-348-1800
Email: mspecwg@einformation.ussf.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/11

What is a breach:

The unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

When is notice required:

- Personal information: First name or first initial and last name in combination with (1) Social Security Number; (2) Drivers License or state identification card number; (3) Account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to any resident's financial account.

Who has to notify:

- A data owner or licensee.
- A person that maintains the data must notify the owner or licensee.

Who has to be notified:

- Any individual who is a resident of this state whose personal information was, or is reasonably believed to have been intentionally acquired by an unauthorized person through a breach of security.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- Without unreasonable delay subject to the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the data system.
- Notice may be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security and the law enforcement agency has made a request that the notification be delayed.

Permitted delivery of notice:

- Written notice.
- Electronic notice, if the person's primary means of communication with the affected individuals is by electronic means or if electronic notice is consistent with E-Sign requirements.
- Telephonic notice.
- Substitute notice may be done if cost of providing notice exceeds \$5,000 or number of persons exceeds 5,000 or sufficient contact information is not available. All of the following must be done: (i) email; (ii) conspicuous web site posting; and (iii) notice to major statewide media, including newspapers, radio and television.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.

STATUTORY:

- Any person that maintains a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or federal functional regulator, as defined in 15 U.S.C. 6809(2), shall be deemed to be in compliance provided the person notifies affected individuals accordingly.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person or business maintains its own notification procedures consistent with the timing requirements of state law; and if the person or business notifies affected individuals in accordance with its policies.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

STATUTE CITATION

H.B. 583

Original bill text:

<http://billstatus.ls.state.ms.us/documents/2010/pdf/HB/0500-0599/HB0583SG.pdf>

Statutory code:

Not yet available.

ATTORNEY GENERAL

Jim Hood, Esquire

Attorney General of Mississippi

Department of Justice

P.O. Box 220, Jackson, MS 39205

601-359-3680

FBI

Jackson

1220 Echelon Parkway

Jackson, Mississippi 39213

<http://jackson.fbi.gov>

601-948-5000

E-mail: Fbijn@leo.gov

SECRET SERVICE

Jackson

601-965-4436

SUMMARY OF LAW - EFFECTIVE DATE - 7/28/09

What is a breach:

- The unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.

When is notice required:

- Personal information: an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable: (a) Social Security number; (b) Driver's license number or other unique identification number created or collected by a government body; (c) Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; (d) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (e) Medical information; or (f) Health insurance information.

Who has to notify:

- A data owner or licensee.
- A person that maintains the data must notify the owner or licensee.

Who has to be notified:

- The individual.
- The Attorney General's office and all national Consumer Reporting Agencies in the event that notice is provided to more than 1,000 consumers.

Required contents of notice:

- The incident in general terms.
- The type of personal information that was obtained as a result of the breach of security.
- A telephone number that the affected consumer may call for further information and assistance, if one exists.
- Contact information for Consumer Reporting Agencies.
- Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

Timing of notice:

- Notification may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the person documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation.
- Notice is required without unreasonable delay after the law enforcement agency communicates to the person its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

Permitted delivery of notice:

- Written notice.
- Electronic notice, if electronic notice is consistent with E-Sign requirements.
- Telephonic notice, if such contact is made directly with the affected consumers.
- Substitute notice may be done if cost of providing notice exceeds \$100,000 or number of persons exceeds 150,000 or sufficient contact information is not available or affected customers are unidentifiable. All of the following must be done: (i) email; (ii) Web site posting; and (iii) notice to applicable local or statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notification is not required if it is determined that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years.

STATUTORY:

- A person that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with notification requirements if the person notifies affected consumers in accordance with the maintained procedures when a breach occurs.
- A financial institution is in compliance if it is (a) Subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice; or (b) Subject to and in compliance with the National Credit Union Administration regulation; or (c) Subject to and in compliance with the provisions of Title V of the Gramm-Leach-Bliley (GLB) Financial Modernization Act of 1999.

EXISTING POLICY:

- A person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with notice requirements if the person notifies affected consumers in accordance with its policies in the event of a breach of security of the system.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the personal information is encrypted or rendered unreadable or unusable by any other method or technology.

STATUTE CITATION

H.B. 62; cleared for the governor's desk on 5-29-09

Original bill text:

<http://www.house.mo.gov/billtracking/bills091/biltxt/truly/HB0062T.HTM>

Statutory code:

<http://www.moga.mo.gov/statutes/C400-499/4070001500.HTM>

ATTORNEY GENERAL

Chris Koster, Esquire

Attorney General Missouri
Supreme Court Building
207 W. High Street
Jefferson City, MO 65101
573-751-3321

FBI

Kansas City
1300 Summit
Kansas City, Missouri 64105-1362
<http://kansascity.fbi.gov>
816-512-8200
E-mail: Kansas.city@ic.fbi.gov

St. Louis

2222 Market Street
St. Louis, Missouri 63103-2516
<http://stlouis.fbi.gov>
314-589-2500
E-mail: Stlouis@ic.fbi.gov

SECRET SERVICE

Kansas City
816-460-0600
Springfield
417-864-8340
St. Louis
314-539-2238

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 3/1/06

What is a breach:

The unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information and causes or is reasonably believed to cause loss or injury.

When is notice required:

- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license, identification card number, or tribal identification card number; (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to any resident's financial account.

Who has to notify:

- A data owner or licensee or insurance-support organization.
- A person that maintains the data must notify the owner or licensee.

Who has to be notified:

- The individual.
- Coordination with Credit Reporting Agency required if notice suggests, indicates, or implies that the individual may obtain a copy of their credit report.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation and requests a delay in notification. Notification is required after the law enforcement agency determines that it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach, identify individuals affected, and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Telephonic.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to applicable local or statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if no loss or injury was caused or is reasonably believed to be caused.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person or business maintains its own notification procedures that do not unreasonably delay notice if the person or business notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition by an employee or agent of the person or business for the purposes of the person or business, provided that the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the personal information is encrypted.

STATUTE CITATION

Mont. Code Ann. § 30-14-1704

Mont. Code Ann. § 33-19-321

Original bill text:

<http://data.opi.mt.gov/bills/2005/billhtml/HB0732.htm>

Statutory code:

<http://data.opi.mt.gov/bills/mca/30/14/30-14-1704.htm>;

<http://data.opi.mt.gov/bills/mca/33/19/33-19-321.htm>

ATTORNEY GENERAL

Steve Bullock, Esquire

Attorney General of Montana

Department of Justice

P.O.Box 201401

Helena, MT 59620-1401

406-444-2026

FBI

Salt Lake City, UT * *FBI field office Salt*

Lake City, UT also covers Montana

257 East 200 South

Suite 1200

Salt Lake City, UT 84111-2048

801-579-1400

<http://saltlakecity.fbi.gov>

E-mail: SaltLakeCity@ic.fbi.gov

SECRET SERVICE

Billings

406-245-8585

CONSUMER CREDIT REPORTING

AGENCIES CONTACT

INFORMATION:

Experian®: Send an e-mail to

BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to

businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to

fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 7/14/06

What is a breach:

The unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information.

When is notice required:

- Computerized data containing personal information: unencrypted, unredacted, or otherwise unaltered by any method or technology in such a manner that name or data is unreadable.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account; (4) unique electronic identification card number or routing code, in combination with any required security code, access code, or password; or (5) unique biometric data.

Who has to notify:

- A data owner or licensee.
- A person that maintains computerized data must notify and cooperate with the owner or licensee.

Who has to be notified:

- The individual.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- As soon as possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it will no longer impede the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Telephonic.
- Substitute notice may be done if cost of providing notice exceeds \$75,000 or number of persons exceeds 100,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.
- Substitute notice may be done if the individual/commercial entity has 10 employees or fewer and the cost of providing notice exceeds \$10,000. All of the following must be done: (i) email; (ii) paid advertisement in a local newspaper that is distributed in the geographic area in which the individual/commercial entity is located, of sufficient size to cover at least 1/4 page and published in the newspaper at least once a week for 3 consecutive weeks; (iii) web site posting; and (4) notification to major media outlets in the geographic area in which the individual/commercial entity is located.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after a reasonable and prompt investigation in good faith, it is determined that the use of personal information for an unauthorized purpose is not likely to occur.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are regulated by state or federal law and procedures are maintained pursuant to laws, rules, regulations, or guidelines established by the primary or functional state or federal regulator; and if notice is in accordance with the maintained procedures.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person or a commercial entity maintains its own notice procedures consistent with the timing requirements of state law, if the person or the commercial entity notifies affected individuals in accordance with its procedures.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition by an employee or agent of a person or a commercial entity for the purposes of the person or the commercial entity if the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the personal information is encrypted.

LEGAL PROCESS:

- Notice is not required if disclosure is made pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency.

STATUTE CITATION

R.R.S. Neb. § 87-801 through § 87-807

Original bill text:

<http://www.legislature.ne.gov/FloorDocs/99/PDF/Slip/LB876.pdf>

Statutory code:

<http://uniweb.legislature.ne.gov/laws/browse-chapters.php?chapter=87>

ATTORNEY GENERAL

Jon Bruning, Esquire
Attorney General of Nebraska
State Capitol
P.O Box 98920
2115 State Capitol
Lincoln, NE 68509
402-471-2682

FBI

Omaha
10755 Burt Street
Omaha, Nebraska 68114-2000
402-493-8688
<http://omaha.fbi.gov>
E-mail: Omaha@ic.fbi.gov

SECRET SERVICE

Omaha
402-965-9670

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with “Database Compromise” as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/06; AMENDMENTS EFFECTIVE - 1/1/10

What is a breach:

The unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or identification card number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A data owner or licensee.
- A person that maintains computerized data must notify the owner or licensee.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 75,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED**STATUTORY:**

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are subject to and in compliance with the privacy and security provisions of the Gramm-Leach-Bliley Act (GLB).

EXISTING POLICY:

- Certain notice requirements may be satisfied if the data collector maintains its own notification policies and procedures that are consistent with the timing requirements of state law; and if the data collector notifies affected individuals in accordance with its policies and procedures.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public.

ENCRYPTION:

- Notice is not required if in compliance with the current version of the Payment Card Industry (PCI) Data Security Standard.
- Notice is not required if no transfer of any personal information through an electronic, non-voice transmission other than a facsimile to a person outside of the secure system of the data collector.
- Notice is not required if no movement of any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor.
- Notice is not required if the personal information is encrypted and the breach is not caused by gross negligence or intentional misconduct of the data collector, its officers, employees, or agents.
- Encryption is defined as the protection of data in electronic or optical form, in storage or in transit, using:
 1. An encryption technology that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and
 2. Appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body, including, but not limited to, the National Institute of Standards and Technology.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

- Notice is not required if the data collector is in compliance with the PCI DSS and the breach is not caused by gross negligence or intentional misconduct of the data collector, its officers, employees, or agents.

STATUTE CITATION

Nev. Revised Statutes 52 § 603A.220

Original bill text:

http://www.leg.state.nv.us/Session/73rd2005/bills/SB/SB347_EN.pdf

Amendment text:

http://www.leg.state.nv.us/75th2009/Bills/SB/SB227_EN.pdf

Statutory Code:

<http://www.leg.state.nv.us/NRS/NRS-603A.html#NRS603A220>

ATTORNEY GENERAL

Catherine Cortez Masto, Esquire
Attorney General of Nevada
Old Supreme Court Building
100 N. Carson Street
Carson City, NV 89701
775-684-1100

FBI

Las Vegas
John Lawrence Bailey Building
1787 West Lake Mead Boulevard
Las Vegas, Nevada 89106-2135
<http://lasvegas.fbi.gov>
702-385-1281
E-mail: Lasvegas@ic.fbi.gov

SECRET SERVICE

Reno
775-784-5354
Las Vegas
702-868-3000

Electronic Crimes Task Force
Las Vegas
702-388-6571
Email: lasectf@einformation.usss.gov

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/07

What is a breach:

Unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or government identification number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.

Who has to notify:

- A person doing business in this state that owns or licenses computerized data that includes personal information.
- A person that maintains computerized data must notify and cooperate with the owner or licensee.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice.
- The primary regulatory authority for any person engaged in trade or commerce. All other persons shall notify the Attorney General's office.

Required contents of notice:

- A description of the incident in general terms.
- The approximate date of breach.
- The type of personal information obtained as a result of the security breach.
- The telephonic contact information of the person subject to this section.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation or jeopardize national or homeland security.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if the business' primary means of communication is electronic.
- Telephonic, provided that a log of each such notification is kept by the person or business who notifies affected persons.
- Substitute notice may be done if cost of providing notice exceeds \$5,000 or number of persons exceeds 1,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, it is determined that misuse of the information has not occurred or is not reasonably likely to occur.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they maintain procedures pursuant to laws, rules, regulations, or guidelines issued by a state or federal regulator; and if notice is in accordance with such laws, rules, regulations, or guidelines.
- Notice is not required to credit reporting agencies under the statute if the entity is subject to and in compliance with Title V of the Gramm-Leach-Bliley Act (GLB).

EXISTING POLICY:

- Certain notice requirements may be satisfied if the person maintains internal notification procedures maintained as part of an information security policy for the treatment of personal information.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business, provided that the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the personal information is encrypted.

STATUTE CITATION

RSA 359-C:19 through 359-C:21

Original bill text:

<http://www.gencourt.state.nh.us/legislation/2006/HB1660.html>

Amendment text:

<http://www.gencourt.state.nh.us/legislation/2010/HB1613.html>

Statutory code:

<http://www.gencourt.state.nh.us/rsa/html/NHTOC/NHTOC-XXXI-359-C.htm>
(see indicated sections C:19-C-21)

ATTORNEY GENERAL

Michael Delaney, Esquire
Attorney General of New Hampshire
State House Annex
33 Capitol Street
Concord, NH 03301-6397
603-271-3658

FBI

Boston, MA * *FBI field office Boston, MA also covers New Hampshire*
One Center Plaza
Suite 600
Boston, Massachusetts 02108
<http://boston.fbi.gov>
617-742-5533
E-mail: Boston@ic.fbi.gov

SECRET SERVICE

Manchester
603-626-5631

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/06

What is a breach:

Unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable and that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or state identification number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.
- Dissociated data that, if linked, would constitute personal information and if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Who has to notify:

- A business that conducts business in New Jersey, or any public entity that complies or maintains computerized records that include personal information.
- A business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- The Division of State Police in the Department of Law and Public Safety for investigation or handling, including dissemination or referral to other appropriate law enforcement entities, in advance of the disclosure to the individual.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal or civil investigation. Notification is required after the law enforcement agency determines that disclosure will not compromise the investigation and notifies that business or public entity.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

Regulatory Authority

- The Director of the Division of Consumer Affairs in the Department of Law and Public Safety, in consultation with the Commissioner of Banking and Insurance, shall promulgate regulations pursuant to the "Administrative Procedure Act," P.L.1968,34 c.410 (C.52:14B-1 et seq.), necessary to effectuate these requirements.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if it is established that misuse of the information is not reasonably possible.
- The determination must be documented in writing for five years.

EXISTING POLICY:

- Notice is not required if a business or public entity maintains its own notification procedures consistent with the requirements of state law, and if the business or public entity notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media.

ENCRYPTION:

- Notice is not required if the personal information is encrypted or rendered unreadable or unusable by any other method or technology.

STATUTE CITATION

N.J. Permanent Statutes 56 § 8-163

Original bill text:

http://www.njleg.state.nj.us/2004/Bills/A3500/4001_R1.PDF

Statutory code:

http://lis.njleg.state.nj.us/cgi-bin/om_isapi.dll?clientID=25539368&Depth=2&depth=2&expandheadings=on&headingswithhits=on&hitsperheading=on&infobase=statutes.nfo&record={17FC0}&softpage=Doc_Frame_PG42

ATTORNEY GENERAL

Paula T. Dow, Esquire

Attorney General of New Jersey
Richard J. Hughes Justice Complex
25 Market Street, P.O. Box 080
Trenton, NJ 08625
609-292-8740

FBI

Newark
Claremont Tower
11 Centre Place
Newark, New Jersey 07102-9889
<http://newark.fbi.gov>
973-792-3000

SECRET SERVICE

Atlantic City
609-487-1300

Newark
973-971-3100

Trenton
609-989-2008

Electronic Crimes Task Force
New York/New Jersey
718-840-1220
Fax: 718-840-1229
E-mail: nyectf@usss.dhs.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 12/7/05

What is a breach:

Unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business that was, or is reasonably believed to have been, acquired by a person without valid authorization.

When is notice required:

- Computerized data containing personal information: unencrypted or encrypted with an encryption key that has also been acquired.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license or non-driver identification card number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual financial account.
- Any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.

Who has to notify:

- A person or business which owns or licenses computerized data which includes private information.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- The nationwide credit reporting agencies must be notified if more than 5,000 individuals receive notice at one time.
- The state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination.

Required contents of notice:

- Contact information for the person or business making the notification.
- A description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it does not compromise such investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if person to who notice is required has expressly consented and a log of each such notification is kept by the person or business who notifies affected persons in such form.
- Telephonic, provided that a log of each such notification is kept by the person or business who notifies affected persons.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if it is determined that information was not, or is not reasonably believed to have been, acquired by a person without valid authorization.
- The following factors, among others, may be considered in determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization:
 - (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
 - (2) indications that the information has been downloaded or copied; or
 - (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the business for the purposes of the business, provided that the private information is not used or subject to unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information which is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the personal information is encrypted and the encryption key has not also been acquired.

STATUTE CITATION

General Business Law Article 39-F,
Sec. 899-AA

Original bill text:

[http://public.leginfo.state.ny.us/
menugetf.cgi](http://public.leginfo.state.ny.us/menugetf.cgi)

(Search Bill No. S03492A in 2005 –
check the “text” box to access the bill
text)

Statutory code:

[http://www.cscic.state.ny.us/security/
securitybreach/NYS-General-Business-
Law-899-AA-4-08-10.pdf](http://www.cscic.state.ny.us/security/securitybreach/NYS-General-Business-Law-899-AA-4-08-10.pdf)

ATTORNEY GENERAL

Eric Schneiderman, Esquire
Attorney General of New York
Department of Law
The Capitol, 2nd Floor
Albany, NY 12224
518-474-7330

SECURITY BREACH NOTIFICATION

Consumer Frauds & Protection Bureau
120 Broadway-3rd Floor
New York, NY 10271
Fax: 212-416-6003
E-mail: [breach.security@oag.state.
ny.us](mailto:breach.security@oag.state.ny.us)

New York State Office of CyberSecurity
& Critical Infrastructure Coordination
(CSCIC)

SECURITY BREACH NOTIFICATION

30 South Pearl Street, Floor P2
Albany, NY 12207
Fax: 518-474-9090
E-mail: info@cscic.state.ny.us

New York State Consumer Protection
Board (CPB):

SECURITY BREACH NOTIFICATION

5 Empire State Plaza, Suite 2101
Albany, NY 12223
Fax: 518-474-2474
Email: [security_breach_notification@
consumer.state.ny.us](mailto:security_breach_notification@consumer.state.ny.us)

FBI

Albany
200 McCarty Avenue
Albany, New York 12209
<http://albany.fbi.gov>
518-465-7551

Buffalo
One FBI Plaza
Buffalo, New York 14202-2698
<http://buffalo.fbi.gov>
716-856-7800
E-mail: Buffalo.bf@ic.fbi.gov

New York
26 Federal Plaza, 23rd. Floor
New York, New York 10278-0004
<http://newyork.fbi.gov>
212-384-1000
E-mail: Ny1@ic.fbi.gov

SECRET SERVICE

Albany
518-436-9600

JFK
718-553-0911

New York
718-840-1000

Melville
631-293-4028

Rochester
585-232-4160

Syracuse
315-448-0304

White Plains
914-682-6300

Electronic Crimes Task Force
New York/New Jersey
718-840-1220
Fax: 718-840-1229
E-mail: nyectf@usss.dhs.gov

Electronic Crimes Task Force
Buffalo
716-551-4401
Email: bufactf@einformation.usss.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to
[BusinessRecordsVictimAssistance@
Experian.com](mailto:BusinessRecordsVictimAssistance@Experian.com).

Equifax®: Send an e-mail to
businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to
fvad@transunion.com, with
“Database Compromise” as the
subject.

SUMMARY OF LAW - EFFECTIVE DATE - 12/1/05; AMMENDMENTS EFFECTIVE 10/1/09

What is a breach:

An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer.

Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach.

When is notice required:

- Unencrypted records or data containing personal information.
- Encrypted records or data containing personal information when the confidential process or key has been accessed or acquired.
- Personal information: First name or first initial and last name in combination with (1) Social Security number or employer taxpayer identification numbers; (2) drivers license or state identification card number or passport number; (3) checking account numbers; (4) savings account numbers; (5) credit card numbers; (6) debit card numbers; (7) personal identification (PIN) code; (8) digital signatures; (9) any other numbers or information that can be used to access a person's financial resources; (10) biometric data; or (11) fingerprints.

Personal information also may include first name or first initial and last name in combination with parent's legal surname prior to marriage, passwords, or electronic identification numbers, electronic mail names or addresses, internet account numbers, or internet identification names if this information would permit access to a person's financial account or resources.

Who has to notify:

- A business that owns or licenses personal information of residents of North Carolina.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- If notice to any affected person pursuant to this section, notice without unreasonable delay to the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected, steps taken to investigate the breach, steps taken to prevent a similar breach, and information regarding the timing, distribution, and content of the notice.

Required contents of notice:

The notice shall be clear and conspicuous and include all of the following:

- A description of the incident in general terms.
- A description of the type of personal information that was subject to the unauthorized access and acquisition.
- A description of the general acts of the business to protect the personal information from further unauthorized access.
- A telephone number for the business that the person may call for further information and assistance, if one exists.
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.
- The toll-free numbers and addresses for the major consumer reporting agencies.
- The toll-free numbers, addresses, web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

Timing of notice:

- Without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation or jeopardize national or homeland security. Notification is required after the law enforcement agency communicates a determination that it will no longer impede an investigation or jeopardize national or homeland security.
- Notification may be delayed to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Permitted delivery of notice:

- Written.
- Electronic, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically and if electronic notice is consistent with E-Sign requirements.
- Telephonic, provided that contact is made directly with the affected persons.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if illegal use of the information has not occurred or is not reasonably likely to occur or does not create a material risk of harm.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number.
- Notice is not required if the information is information made lawfully available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the personal information is encrypted and the encryption key has not also been acquired.

STATUTE CITATION

N.C. General Statutes Ann. § 75-65

Original bill text:

<http://www.ncleg.net/Sessions/2005/Bills/Senate/HTML/S1048v6.html>

Amendment text:

<http://www.ncleg.net/Sessions/2009/Bills/Senate/HTML/S1017v7.html>

Statutory code:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-65.html

ATTORNEY GENERAL

Roy Cooper, Esquire

Attorney General of North Carolina

Department of Justice

P.O Box 629

Raleigh, NC 27602-0629

919-716-6400

Consumer Protection Division

NC Attorney General's Office

9001 Mail Service Center

Raleigh, NC 27699-9001

919-716-6000

919-716-6050 (fax)

FBI

Charlotte

7915 Microsoft Way

Charlotte, North Carolina 28273

<http://charlotte.fbi.gov>

(704) 672-6100

E-mail: Charlotte.public@ic.fbi.gov

SECRET SERVICE

Greensboro

336-547-4180

Raleigh

919-790-2834

Wilmington

910-313-3043

Electronic Crimes Task Force

Charlotte

704-442-8370

Email: ctectf@einformation.usss.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to

BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to

businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to

fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/05

What is a breach:

Unauthorized acquisition of computerized data containing personal information that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted or not secured by encryption or by any other method or technology that renders the electronic files, media, or data bases unreadable or unusable.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) operator's license number; (3) non-driver color photo identification card number assigned to the individual by the Department of Transportation; (4) the individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts; (5) date of birth; (6) maiden name of the individual's mother; (7) identification number assigned to the individual by the individual's employer; or (8) digitized or other electronic signature.

Who has to notify:

- A person that conducts business in this state, and that owns or licenses computerized data that includes personal information.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it will no longer compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the integrity of the data system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person maintains its own notification procedures consistent with the timing requirements of state law; and if the person notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good-faith acquisition of personal information by an employee or agent of the person, if the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the personal information is encrypted.

STATUTE CITATION

N.D. Century Code 51 § 30-02

Original bill text:

<http://www.legis.nd.gov/assembly/59-2005/bill-text/FRBS0500.pdf>

Statutory code:

<http://www.legis.nd.gov/cencode/t51c30.pdf>

ATTORNEY GENERAL

Wayne Stenehjem, Esquire
Attorney General of North Dakota
State Capitol
600 E. Boulevard Avenue
Dept. 125
Bismarck, ND 58505-0040
701-328-2210

FBI

Minneapolis * *FBI field office Minneapolis, MN also covers North Dakota*
111 Washington Avenue South
Suite 1100
Minneapolis, Minnesota 55401-2176
<http://minneapolis.fbi.gov>
(612) 376-3200

SECRET SERVICE

Fargo
701-239-5070

SUMMARY OF LAW - EFFECTIVE DATE - 2/17/06

What is a breach:

Unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.

When is notice required:

- Computerized data containing personal information: unencrypted, unredacted, or unaltered by any method or technology in such manner that the data is unreadable.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or identification card number; or (3) account number or credit card number or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

Who has to notify:

- A state agency, an agency of a political subdivision, or a person, including a business entity that does business in Ohio.
- A person pursuant to a contract entered into prior to the date of the breach.
- A person that, on behalf of or at the direction of another person, is the custodian of or stores personal information must notify the owner or licensee of the information.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice in a single occurrence.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible but not later than 45 days following discovery/notification of the breach.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation or jeopardize homeland or national security. Notification is required after the law enforcement agency determines that it will not compromise the investigation or jeopardize homeland or national security.
- Notification may be delayed to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the integrity of the data system.

Permitted delivery of notice:

- Written.
- Electronic, if the person's primary method of communication with the affected resident is by electronic means.
- Telephonic.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media, to the extent that cumulative total of the readership, viewing audience, or listening audience so notified equals or exceeds 75% of the state population.
- Substitute may be done if the business entity has 10 employees or fewer and the cost exceeds \$10,000. All of the following must be done: (i) paid advertisement of sufficient size to cover at least 1/4 page in a local newspaper that is distributed in the geographic area in which the business entity is located, and shall be published at least once a week for 3 consecutive weeks; (ii) web site posting; and (3) notification to major media outlets in the geographic area in which the business entity is located.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if the access and acquisition by the unauthorized person has not caused or reasonably is believed will not cause a material risk of identity theft or other fraud.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are required by and subject to examination by the functional government regulatory agency for compliance with federal law.
- Provisions do not apply to entities subject to the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition by an employee or agent of the person for the purposes of the person, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed:
 - (i) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television;
 - (ii) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media;
 - (iii) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation; or
 - (iv) Any type of media similar in nature to any item, entity, or activity identified in this section.

ENCRYPTION:

- Notice is not required if the personal information is encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable.

STATUTE CITATION

Ohio Revised Code 13 § 1349.19

Original bill text:

http://www.legislature.state.oh.us/bills.cfm?ID=126_HB_104

Statutory code:

<http://codes.ohio.gov/orc/1349.19>

ATTORNEY GENERAL

Mike DeWine, Esquire

Attorney General of Ohio

State Office Tower

30 E. Broad Street, 14th Floor

Columbus, OH 43215

614-466-4320

FBI

Cincinnati

550 Main Street

Suite 9000

Cincinnati, Ohio 45202-8501

<http://cincinnati.fbi.gov>

513-421-4310

Cleveland

Federal Office Building

1501 Lakeside Avenue

Cleveland, Ohio 44114

<http://cleveland.fbi.gov>

216-522-1400

E-mail: Cleveland.cv@ic.fbi.gov

SECRET SERVICE

Akron

330-761-0544

Cincinnati

513-684-3585

Columbus

614-469-7370

Dayton

937-222-2013

Toledo

419-259-6434

Electronic Crimes Task Force

Cleveland

216-706-4365

Fax: 216-706-4445

Email: Cleectf@einformation.ussf.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to

BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to

businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to

fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 11/1/08

What is a breach:

Unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.

When is notice required:

- Computerized data containing personal information: unencrypted or unredacted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or identification card number; or (3) financial account number or credit card number or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to the financial account of a resident.

Who has to notify:

- An individual or entity that owns or licenses computerized data.
- An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license must notify the owner or licensee.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- Without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines and advises the individual or entity that notification will impede a criminal or civil investigation or jeopardize national or homeland security. Notification is required after the law enforcement agency determines that it will no longer impede the investigation or jeopardize national or homeland security.
- Notification may be delayed to determine the scope of the breach and to restore the integrity of the system.

Permitted delivery of notice:

- Written to the postal address in the entity's records.
- Telephonic.
- Electronic.
- Substitute notice may be done if cost of providing notice exceeds \$50,000 or number of persons exceeds 100,000 or sufficient contact information not available. Two of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if it is reasonably believed that the breach has not caused or will not cause, identity theft or other fraud.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are in compliance with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.
- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are in compliance with the notification requirements or procedures pursuant to the rules, regulation, procedures, or guidelines established by the primary or functional federal regulator of the entity.

EXISTING POLICY:

- Certain notice requirements may be satisfied if an entity maintains its own notification procedures consistent with the timing requirements of state law; and if it notifies affected individuals in accordance with its procedures.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition by an employee or agent of an individual or entity for the purposes of the individual or the entity, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

ENCRYPTION:

- Notice is not required if encrypted information is accessed and acquired in encrypted form and if the security breach involves a person without access to the encryption key.

STATUTE CITATION

24 Okl. St. § 161 through 166

[Original bill text:](#)

Not available.

Statutory code:

http://webserver1.lsb.state.ok.us/OK_Statutes/CompleteTitles/os24.rtf

[\(Security Breach Notification provisions begin at page 43 § 161 through 166\)](#)

ATTORNEY GENERAL

Scott Pruitt, Esquire

Attorney General of Oklahoma

313 NE 21st St.

Oklahoma City, OK 73105

405-521-3921

FBI

Oklahoma City

3301 West Memorial Drive

Oklahoma City, Oklahoma 73134

<http://oklahomacity.fbi.gov>

405-290-7770

SECRET SERVICE

Tulsa

918-581-7272

Electronic Crimes Task Force

Oklahoma City

405-810-3000

[Email: okcecw@einformation.uss.gov](mailto:okcecw@einformation.uss.gov)

SUMMARY OF LAW - EFFECTIVE DATE - 10/1/07

What is a breach:

Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the person.

When is notice required:

- Computerized data containing personal information: unencrypted, unredacted, or not rendered unusable by other methods.
- Encrypted data when the encryption key has also been acquired.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or identification card number issued by the Department of Transportation; or (3) financial account number or credit card number or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to a consumer's financial account.
- Personal information: Data when not combined with the first name or first initial and last name and when the data is not rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft.

Who has to notify:

- A person that owns, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals are affected.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

- A description of the incident in general terms.
- The approximate date of the breach of security.
- The type of personal information obtained as a result of the breach of security.
- Contact information of the person subject to this section.
- Contact information for national consumer reporting agencies.
- Advice to the consumer to report suspected identity theft to law enforcement, including the Federal Trade Commission.

Timing of notice:

- The most expeditious time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation and that agency has made a written request that the notification be delayed. Notification is required after the law enforcement agency determines that it will no longer compromise the investigation and notifies the person in writing.
- Notification may be delayed to determine sufficient contact information for the consumers, determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data.

Permitted delivery of notice:

- Written.
- Electronic, if the person's customary method of communication with the consumer is by electronic means or if electronic notice is consistent with E-Sign requirements.
- Telephonic, provided that contact is made directly with the affected consumer.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 350,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide television and newspaper media.

Regulatory Authority:

- The Director of the Department of Consumer and Business Services may adopt rules for the purpose of carrying out notification requirements.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after an appropriate investigation or after consultation with relevant federal, state or local agencies responsible for law enforcement, it is determined that there is no reasonable likelihood of harm.
- The determination must be documented in writing for five years.

STATUTORY:

- Provisions do not apply to entities in compliance with the notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements pursuant to the rules, regulations, procedures, guidance or guidelines established by the primary or functional federal regulator.
- Provisions do not apply to entities in compliance with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security of personal information than that provided by this section.
- Provisions do not apply to entities subject to and in compliance with regulations promulgated pursuant to the Gramm-Leach-Bliley Act (GLB).

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person if the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.

PUBLIC RECORDS:

- Notice is not required if the information consists of information, other than a Social Security number, in a federal, state or local government record that is lawfully made available to the public.

ENCRYPTION:

- Notice is not required if data elements are rendered unusable through encryption, redaction or other methods, and the encryption key has not also been acquired.

STATUTE CITATION

ORS § 646A.600 through § 646A.604
[Original bill text:](http://www.leg.state.or.us/07orlaws/sess0700.dir/0759.htm)
<http://www.leg.state.or.us/07orlaws/sess0700.dir/0759.htm>

[Statutory code:](http://www.leg.state.or.us/ors/646a.html)
<http://www.leg.state.or.us/ors/646a.html>

ATTORNEY GENERAL

John Kroger, Esquire
 Attorney General of Oregon
 Oregon Department of Justice
 1162 Court Street, NE
 Salem, OR 97301
 503-378-4732

FBI

Portland
 Crown Plaza Building
 1500 Southwest 1st Avenue
 Suite 400
 Portland, Oregon 97201-5828
<http://portland.fbi.gov>
 503-224-4181
 E-mail: Portland@ic.fbi.gov

SECRET SERVICE

Portland
 503-326-2162

CONSUMER CREDIT REPORTING AGENCIES CONTACT

INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 6/20/06

What is a breach:

Unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.

When is notice required:

- Computerized data containing personal information: unencrypted or unredacted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or identification card number issued in lieu of a driver's license; or (3) financial account number or credit card number or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to a consumer's financial account.

Who has to notify:

- An entity that maintains, stores or manages computerized data that includes personal information.
- A vendor that maintains, stores or manages computerized data on behalf of another entity must notify the entity on whose behalf the computerized data is maintained, stored or managed. The entity on whose behalf the computerized data is maintained, stored or managed must discharge the remaining notice duties.

Who has to be notified:

- The individual.
- The entity on whose behalf a vendor maintains, stores or manages the data.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- Without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal or civil investigation and the agency has so advised in writing. Notification is required after the law enforcement agency determines that it will no longer compromise the investigation or national or homeland security.
- Notification may be delayed to determine the scope of the breach and to restore the reasonable integrity of the data.

Permitted delivery of notice:

- Written to the last known home address.
- Telephonic, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.
- Electronic, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.
- Substitute notice may be done if cost of providing notice exceeds \$100,000 or number of persons exceeds 175,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are in compliance with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.
- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are in compliance with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the primary or functional Federal regulator.

EXISTING POLICY:

- Certain notice requirements may be satisfied if an entity maintains its own notification procedures consistent with the notice requirements of state law; and if it notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from Federal, State or local government records.

ENCRYPTION:

- Notice is not required if the information is encrypted information and the security breach does not involve a person with access to the encryption key.

STATUTE CITATION

Pa. Statutes 73 § 43-2303

Original bill text:

<http://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=HTM&sessYr=2005&sessInd=0&billBody=S&billTyp=B&billNbr=0712&pn=1410>

Statutory code:

Not available.

ATTORNEY GENERAL

Linda Kelly, Esquire
Attorney General of Pennsylvania
1600 Strawberry Square, 16th Floor
Harrisburg, PA 17120
717-787-3391

FBI

Philadelphia
William J. Green Jr. FOB
600 Arch Street
8th Floor
Philadelphia, Pennsylvania 19106
<http://philadelphia.fbi.gov>
215-418-4000
E-mail: Philadelphia.complaints@ic.fbi.gov

Pittsburgh
3311 East Carson St.
Pittsburgh, Pennsylvania 15203
<http://pittsburgh.fbi.gov>
412-432-4000

SECRET SERVICE

Harrisburg
717-221-4411

Scranton
570-346-5781

Electronic Crimes Task Force
Philadelphia
215-861-3300
Email: phlectf@einformation.usss.gov

Electronic Crimes Task Force
Pittsburgh
412-281-7825
Email: tri-cin@usss.dhs.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 11/4/05; AMENDMENTS EFFECTIVE - 6/19/08

What is a breach:

Any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. This includes both access to the data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings.

When is notice required:

- Personal information: First name or first initial and last name in combination with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code: (1) Social Security number; (2) drivers license number, voter's identification or other official identification; (3) bank or financial account numbers of any type with or without passwords or access code that may have been assigned; (4) names of users and passwords or access codes to public or private information systems; (5) medical information protected by the Health Insurance Portability and Accountability Act (HIPAA); (6) tax information; or (7) work-related evaluations. Neither the mailing nor the residential address is included as protected information.

Who has to notify:

- An entity owning or keeping a database which includes personal information of citizens residing in Puerto Rico.
- An entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens.

Who has to be notified:

- The individual.
- The proprietor, custodian or holder of digital data banks that at the same time contain personal information files of citizens.
- The Department of Consumer Affairs within 10 days.
- A public corporation shall notify the Ombudsman's Office.

Required contents of notice:

Clear and conspicuous:

- Describe the infringement to the system's security in general terms.
- The type of privileged information involved.
- A toll free number or an Internet website that can be used by citizens in order to receive more information or assistance.

Timing of notice:

- As expeditiously as possible.
- Notification may be delayed for the needs of law enforcement agencies to secure possible crime scenes and evidence.
- Notification may be delayed to apply measures needed to restore the system's security.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with the Digital Signatures Act.
- Substitute notice may be done if the cost of notifying all those potentially affected or of identifying them is excessively onerous due to the number of persons affected, to the difficulty in locating all persons or to the economic situation of the enterprise or entity; or if cost of providing notice exceeds \$100,000 or number of persons exceeds 100,000 or sufficient contact information not available. The following two steps must be done: (i) prominent display of an announcement at the entities premises, on the web page of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic, and (ii) a communication to the media informing of the situation and providing information as to how to contact the entity to allow for better follow-up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards that sector.

WHEN IS NOTICE NOT REQUIRED

EXISTING POLICY:

- Notice is not required if an enterprise or entity has institutional information and security policies whose purpose is to provide protection equal or better to the information established in this law.

GOOD FAITH:

- Notice is not required when normally authorized persons or entities have had access and there is no known reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information.

PUBLIC RECORDS:

- Notice is not required if the information consists of public documents that are available to the citizens in general.

ENCRYPTION:

- Notice is not required if the personal information had cryptographic keys other than a password.

STATUTE CITATION

10 L.P.R.A. § 4051 et seq.

Original code text:

<http://www.oslpr.org/download/en/2005/A-0111-2005.pdf>

Amendment text:

Law No. 97 not available.

Statutory code:

http://www.michie.com/puertorico/lpext.dll?f=FifLink&t=document-frame.htm&l=jump&iid=3002f40.13b39ea1.0.0&nid=4b81#JD_t10st3c310

ATTORNEY GENERAL

Guillermo Somoza-Colombani, Esquire

Attorney General of Puerto Rico

GPO Box 902192

San Juan, PR 00902-0192

787-721-2900

FBI

San Juan Physical Address

U.S. Federal Bldg.

150 Carlos Chardon Avenue

Suite 526

Hato Rey, Puerto Rico 00918-1716

<http://sanjuan.fbi.gov>

(787) 754-6000

San Juan Mailing Address

PO Box 366269

San Juan, Puerto Rico 00936-6269

SECRET SERVICE

San Juan

787-277-1515

SUMMARY OF LAW - EFFECTIVE DATE - 3/1/06

What is a breach:

Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the state agency or person that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or identification card number; or (3) account number or credit card number or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to a consumer's financial account.

Who has to notify:

- A person that owns, maintains or licenses computerized data that includes personal information.
- A person that maintains computerized unencrypted data that includes personal information that the state agency or person does not own must notify the owner or licensee.

Who has to be notified:

- The individual.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the data system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$25,000 or number of persons exceeds 50,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, after an appropriate investigation or after consultation with relevant federal, state, or local law enforcement agencies, it is determined that the breach has not and will not likely result in a significant risk of identity theft.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they maintain security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, provided such notice is in accordance with the policies.
- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are subject to and examined for, and found in compliance with the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice.
- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are subject to Health Insurance Portability and Accountability Act (HIPAA).

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency, provided that the personal information is not used or subject to further unauthorized disclosure.

ENCRYPTION:

- Notice is not required if the information is encrypted.

STATUTE CITATION

General Laws of R.I. Ann. § 11-49.2-3

Original bill text:

<http://www.rilin.state.ri.us/Billtext/BillText05/HouseText05/H6191.pdf>

Statutory code:

<http://www.rilin.state.ri.us/Statutes/TITLE11/11-49.2/INDEX.HTM>

ATTORNEY GENERAL

Peter Kilmartin, Esquire
Attorney General of Rhode Island
150 S. Main Street
Providence, RI 02903
401-274-4400

FBI

Boston, MA * *FBI Boston, MA also covers Rhode Island*
One Center Plaza
Suite 600
Boston, Massachusetts 02108
<http://boston.fbi.gov>
617-742-5533
E-mail: Boston@ic.fbi.gov

SECRET SERVICE

Providence
401-331-6456

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/09

What is a breach:

Unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident.

When is notice required:

- Computerized data containing personal information: unencrypted, unredacted or not rendered unusable by other methods.
- “Personal identifying information” means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the State, when the data elements are neither encrypted nor redacted: (1) social security number; (2) driver’s license number or state identification card number issued instead of a driver’s license; (3) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident’s financial account; or (4) other numbers or information which may be used to access a person’s financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.

Who has to notify:

- A person conducting business in this state, and owning or licensing computerized data or other data that includes personal identifying information.
- A person that maintains computerized unencrypted data that includes personal information that the state agency or person does not own must notify the owner or licensee.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- The Consumer Protection Division of the Department of Consumer Affairs if more than 1,000 individuals receive notice at one time.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it no longer compromises the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the data system.

Permitted delivery of notice:

- Written.
- Electronic, if the person’s primary method of communication with the individual is by electronic means or if electronic notice is consistent with E-Sign requirements.
- Telephonic notice.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if the illegal use of the information has not occurred or is not reasonably likely to occur or use of the information does not create a material risk of harm.

STATUTORY:

- Certain requirements are inapplicable to banks or financial institutions subject to and in compliance with the privacy and security provision of the Gramm-Leach-Bliley Act (GLB).
- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are subject to and in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person maintains its own notification procedures consistent with the timing requirements of state law; and if the person notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal identifying information by an employee or agent of the person for the purposes of its business; and if the personal identifying information is not used or subject to further unauthorized disclosure.

ENCRYPTION:

- Notice is not required if the information is encrypted or redacted.

STATUTE CITATION

S.C. Code § 39-1-90

Original bill text:

http://www.scstatehouse.gov/sess117_2007-2008/bills/453.htm

Statutory code:

<http://www.scstatehouse.gov/code/t39c001.htm>

ATTORNEY GENERAL

Alan Wilson, Esquire

Attorney General of South Carolina

The Honorable Alan Wilson

P.O Box 11549

Columbia, SC 29211

803-734-3970

FBI

Columbia

151 Westpark Blvd

Columbia, South Carolina 29210-3857

<http://columbia.fbi.gov>

803-551-4200

SECRET SERVICE

Charleston

843-388-0305

Greenville

864-233-1490

Electronic Crimes Task Force

Columbia

803-772-4015

Email: cssectf@einformation.usss.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT

INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/05

What is a breach:

Unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted.
- “Personal identifying information” means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the State, when the data elements are neither encrypted nor redacted: (1) social security number; (2) driver’s license number or state identification card number issued instead of a driver’s license; (3) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident’s financial account; or (4) other numbers or information which may be used to access a person’s financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.

Who has to notify:

- An information holder.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the data system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

STATUTORY:

- Certain provisions are inapplicable to persons subject to Title V of the Gramm-Leach-Bliley Act (GLB).

EXISTING POLICY:

- Certain notice requirements may be satisfied if an information holder maintains its own notification procedures consistent with the timing requirements of state law, and if it notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder; provided, that the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the information is encrypted.

STATUTE CITATION

Tenn. Code 47 § 18-2107

Original bill text:

<http://www.capitol.tn.gov/Bills/104/Bill/HB2170.pdf>

Statutory code:

<http://www.lexisnexis.com/hottopics/tncode/>

ATTORNEY GENERAL

Robert E. Cooper, Jr., Esquire

Attorney General of Tennessee

425 5th Avenue North

P.O. Box 20207

Nashville, TN 37243

615-741-3491

FBI

Knoxville

1501 Dowell Springs Boulevard

Knoxville, Tennessee 37909

<http://knoxville.fbi.gov>

865-544-0751

E-mail: Knoxville@ic.fbi.gov

Memphis

Eagle Crest Bldg.

225 North Humphreys Boulevard

Suite 3000

Memphis, Tennessee 38120-2107

<http://memphis.fbi.gov>

901-747-4300

SECRET SERVICE

Chattanooga

423-752-5125

Knoxville

865-545-4627

Memphis

901-544-0333

Nashville

615-736-5841

CONSUMER CREDIT REPORTING

AGENCIES CONTACT

INFORMATION:

Experian®: Send an e-mail to

BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to

businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to

fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW – EFFECTIVE DATE – 9/1/05; RECODIFIED – 4/1/09;
AMENDMENTS EFFECTIVE 9/1/09; AMENDMENTS EFFECTIVE 9/1/12

What is a breach:

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person that was, or is reasonably believed to have been, accessed by an unauthorized person. This includes data that is encrypted if the person accessing the data has the key required to decrypt the data.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Sensitive personal information:
 - First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or government issued identification number; or (3) account number or credit card number or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account, or
 - Information that identifies an individual and relates to: (1) the physical or mental health or condition of the individual; (2) the provision of health care to the individual; or (3) payment for the provision of health care to the individual.

Who has to notify:

- A person that conducts business in this state and owns or licenses computerized data that includes sensitive personal information.

Who has to be notified:

- Any individual who is a Texas resident or another state that does not require breach notification.
- The owner or licensee of the information.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- As quickly as possible.
- Notification may be delayed if a law enforcement agency request determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the data system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting; and (iii) notice published in or broadcast on major statewide media.

WHEN IS NOTICE NOT REQUIRED

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person maintains its own notification procedures consistent with the timing requirements under state law; and if the person notifies affected individuals in accordance with its policy.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person unless the person uses or discloses the sensitive personal information in an unauthorized manner.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the public from the federal government or a state or local government.

ENCRYPTION:

- Notice is not required if the information is encrypted.

STATUTORY:

- Notice is not required if notice of the breach has been sent to the individual pursuant to the state law where the individual resides.

STATUTE CITATION

Tex. Code of Criminal Procedure 4 § 48.103

Original bill text:

<http://www.legis.state.tx.us/tlodocs/80R/billtext/pdf/HB02278F.pdf#navpanes=0>

Amendment text:

<http://www.legis.state.tx.us/tlodocs/81R/billtext/pdf/HB02004F.pdf>

Amendment text:

<http://www.capitol.state.tx.us/tlodocs/82R/billtext/pdf/HB00300F.pdf#navpanes=0>

Statutory code:

<http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm#521.053>

ATTORNEY GENERAL

Greg Abbott, Esquire
 Attorney General of Texas
 Capitol Station
 P.O. Box 12548
 Austin, TX 78711-2548
 512-463-2100

FBI

Dallas
 One Justice Way
 Dallas, Texas 75220
<http://dallas.fbi.gov>
 972-559-5000
 E-mail: Fbi.dallas@ic.fbi.gov

El Paso
 660 S. Mesa Hills Drive
 El Paso, Texas 79912-5533
<http://elpaso.fbi.gov>
 915-832-5000

Houston
 1 Justice Park Drive
 Houston, Texas 77092
<http://houston.fbi.gov>
 713-693-5000
 E-mail: Houston.Texas@ic.fbi.gov

San Antonio
 5740 University Heights Boulevard
 San Antonio, Texas 78249
<http://sanantonio.fbi.gov>
 210-225-6741
 E-mail: SanAntonio@ic.fbi.gov

SECRET SERVICE

Austin
 512-916-5103
 El Paso
 915-532-2144

Lubbock
 806-472-7347

Mcallen
 956-994-0151

San Antonio
 210-308-6220

Tyler
 903-534-2933

Waco
 254-741-0576

Electronic Crimes Task Force
 Dallas
 972-868-3200
 Email: dalectf@einformation.usss.gov

Electronic Crimes Task Force
 Houston
 713-868-2299
 Email: houectf@einformation.usss.gov

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.
 Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.
 TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/07

What is a breach:

Unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or identification card number; or (3) financial account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to the person's account.

Who has to notify:

- A person who owns or licenses computerized data that includes personal information concerning a Utah resident.
- A person that maintains computerized data on behalf of another must notify and cooperate with the owner or licensee.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines and informs the person that it will no longer impede the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the data system.

Permitted delivery of notice:

- Written by first-class mail.
- Electronic, if the person's primary method of communication with the resident is by electronic means or if electronic notice is consistent with E-Sign.
- Telephonic, including through the use of automatic dialing technology not prohibited by other law.
- Publishing notice of the breach in a newspaper of general circulation.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if an investigation reveals that the misuse of personal information for identity theft or fraud purposes has not occurred, or is not reasonably likely to occur.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are regulated by state or federal law and procedures are maintained under applicable law established by the primary state or federal regulator; and if notice is in accordance with the other applicable law.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person maintains its own notification procedures consistent with the notification requirements of state law; and the person notifies affected individuals in accordance with its information security policy.

GOOD FAITH:

- Notice is not required if acquisition of personal information is by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.

PUBLIC RECORDS:

- Notice is not required if the information consists of information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.

ENCRYPTION:

- Notice is not required if the information is encrypted or protected by another method that renders the data unreadable or unusable.

STATUTE CITATION

Utah Code 13 § 44-202

Original bill text:

<http://le.utah.gov/~2006/bills/sbillenr/sb0069.pdf>

Statutory code:

http://le.utah.gov/~code/TITLE13/htm/13_44_010200.htm;

http://le.utah.gov/~code/TITLE13/htm/13_44_020200.htm

ATTORNEY GENERAL

Mark Shurtleff, Esquire

Attorney General of Utah

Office of the Attorney General

P.O. Box 142320

Salt Lake City, UT 84114-2320

801-538-9600

FBI

Salt Lake City

257 East 200 South

Suite 1200

Salt Lake City, Utah 84111-2048

<http://saltlakecity.fbi.gov>

801-579-1400

E-mail: SaltLakeCity@ic.fbi.gov

SECRET SERVICE

Salt Lake City

801-524-5910

SUMMARY OF LAW - EFFECTIVE DATE - 1/1/07

What is a breach:

Unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.

When is notice required:

- Computerized data containing personal information: unencrypted, unredacted or not protected by another method that renders the data unreadable or unusable by unauthorized persons.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) motor vehicle operator's license number or non-driver identification card number; (3) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; or (4) account passwords or personal identification numbers or other access codes for a financial account.

Who has to notify:

- A data collector.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- The Vermont Attorney General or to the Department of Banking, Insurance, Securities, and Health Care Administration (BISHCA) if licensed or registered with the department.

Required contents of notice:

- The incident in general terms.
- The type of personal information subject to the unauthorized access or acquisition.
- The general acts of the business to protect the personal information from further unauthorized access or acquisition.
- A toll-free telephone number that the consumer may call for further information and assistance.
- Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede an investigation or a national or homeland security investigation or jeopardize public safety or national or homeland security interests. Notification is required after the law enforcement agency sends a written communication withdrawing its request.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.

Permitted delivery of notice:

- Written to the consumer's residence.
- Electronic, if no contact information, primary method of communication with the consumer is by electronic means, does not request or contain a hypertext link to a request that the consumer provide personal information, and conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or if electronic notice is consistent with E-Sign requirements.
- Telephonic, provided that telephonic contact is made directly with each affected consumer, and the telephonic contact is not through a prerecorded message.
- Substitute notice may be done if cost of providing notice exceeds \$5,000 or number of persons exceeds 5,000 or sufficient contact information not available. All of the following must be done: (i) web site posting and (ii) notice to major statewide and regional media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if the data collector establishes that misuse of personal information is not reasonably possible.
- The data collector must provide notice of the determination and a detailed explanation to the Vermont Attorney General or to the Department of Banking, Insurance, Securities, and Health Care Administration (BISHCA) if licensed or registered with the department.

STATUTORY:

- Notice to credit reporting agencies is not required if licensed or registered under Title 8 by the Department of Banking, Insurance, Securities, and Health Care Administration (BISHCA).
- Exemptions from certain requirements for persons subject to:
 - The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice; or
 - The National Credit Union Administration Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice.

GOOD FAITH:

- Notice is not required if there has been a good faith but unauthorized acquisition or access of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the information is encrypted.

STATUTE CITATION

9 V.S.A. § 2430 and 9 V.S.A. § 2435

Original bill text:

<http://www.leg.state.vt.us/docs/legdoc.cfm?URL=/docs/2006/acts/ACT162.HTM>

Statutory code:

[http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=09&Chapter=062&Section=02430;](http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=09&Chapter=062&Section=02430)
<http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=09&Chapter=062&Section=02435>

ATTORNEY GENERAL

William H. Sorrell, Esquire
 Attorney General of Vermont
 109 State Street
 Montpelier, VT 05609-1001
 802-828-3171

FBI

Albany, NY * *FBI field office Albany, NY also covers Vermont*
 200 McCarty Ave
 Albany, NY
 518-465-7551
<http://albany.fbi.gov>

SECRET SERVICE

Burlington
 802-651-4091

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW

What is a breach:

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Personal information: (1) Social Security number; (2) drivers license number; or (3) account number, credit card number or debit card number in combination with any required security code, access code, or password that permit access to an individual's financial account.

Who has to notify:

- A person or business that maintains the information.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notice must be made after the law enforcement agency determines that it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the data system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$100,000 or number of persons exceeds 50,000 or sufficient contact information not available. All of the following must be done: (i) web site posting and (ii) notice to major territory-wide media.

WHEN IS NOTICE NOT REQUIRED

EXISTING POLICY:

- Certain notice requirements may be satisfied if an agency maintains its own notification procedures consistent with the timing requirements of this law; and if the agency notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the person/business for the purposes of the person/business if the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the information is encrypted.

STATUTE CITATION

14 V.I.C. § 2208

[Original bill text:](#)

[No bill text found.](#)

[Statutory code:](#)

<http://www.lexisnexis.com/hottopics/vicode/>

ATTORNEY GENERAL

Vincent Frazer, Esquire

Attorney General of Virgin Islands

Department of Justice

G.E.R.S. Complex 488-50C Kronprinsdens Gade

St. Thomas, VI 00802

340-774-5666

FBI

San Juan Physical Address

U.S. Federal Bldg.

150 Carlos Chardon Avenue

Suite 526

Hato Rey, Puerto Rico 00918-1716

<http://sanjuan.fbi.gov>

787-754-6000

San Juan Mailing Address

PO Box 366269

San Juan, Puerto Rico 00936-6269

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/08

What is a breach:

Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth.

When is notice required:

- Computerized data containing personal information: unencrypted or unredacted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or identification card number issued in lieu of a drivers license number; or (3) financial account number or credit card number or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

Who has to notify:

- An individual or entity that owns or licenses computerized data that includes personal information.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- The Office of the Attorney General.

Required contents of notice:

- The incident in general terms.
- The type of personal information that was subject to the unauthorized access and acquisition.
- The general acts of the individual or entity to protect the personal information from further unauthorized access.
- A telephone number that the person may call for further information and assistance, if one exists.
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Timing of notice:

- Without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines and advises the individual/entity that it will impede a criminal or civil investigation or homeland or national security. Notification is required after the law enforcement agency determines that it will no longer impede the investigation or jeopardize national or homeland security.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written to the last known postal address in the individual's/entity's records.
- Telephonic.
- Electronic.
- Substitute notice may be done if cost of providing notice exceeds \$50,000 or number of persons exceeds 100,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting and (iii) notice to major statewide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if it is reasonably believed that the breach has not caused or will not cause, identity theft or another fraud.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are subject to Title V of the Gramm-Leach-Bliley Act (GLB) and maintain breach notification procedures in accordance with the Gramm-Leach-Bliley Act (GLB) requirements.
- Entities are deemed to be in compliance with some or all of the state statute’s requirements if they are in compliance with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the primary or functional state or federal regulator.

EXISTING POLICY:

- Certain notice requirements may be satisfied if an entity maintains its own notification procedures consistent with the timing requirements of state law; and if the entity notifies affected individuals in accordance with its procedures.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition by an employee or agent of an individual or entity for the purposes of the individual or entity, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

ENCRYPTION:

- Notice is not required if the information is encrypted and the security breach does not involve a person with access to the encryption key.

STATUTE CITATION

Va. Code Ann. § 18.2-186.6

Original bill text:

<http://leg1.state.va.us/cgi-bin/legp504.exe?081+ful+SB307ER>

Statutory code:

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-186.6>

ATTORNEY GENERAL

Kenneth T. Cuccinelli, Esquire

Attorney General of Virginia

900 E. Main Street
Richmond, VA 23219

804-786-2071

FBI

Norfolk

150 Corporate Boulevard
Norfolk, Virginia 23502-4999

<http://norfolk.fbi.gov>

757-455-0100

E-mail: Norfolk_FO@ic.fbi.gov

Northern Virginia, contact the
Washington Field Office.

Washington Metropolitan Field Office
601 4th Street, N.W.

Washington, D.C. 20535-0002

<http://washingtondc.fbi.gov>

202-278-2000

E-mail: washington.field@ic.fbi.com

Richmond

1970 E. Parham Road
Richmond, Virginia 23228

<http://richmond.fbi.gov>

804-261-1044

E-mail: Richmond@ic.fbi.gov

SECRET SERVICE

Norfolk

757-441-3200

Richmond

804-592-3086

Roanoke

540-857-2208

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to

BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to

businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to

fvad@transunion.com, with “Database
Compromise” as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 7/24/05

What is a breach:

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business that was, or is reasonably believed to have been, accessed by an unauthorized person.

When is notice required:

- Computerized data containing personal information: unencrypted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or identification card number; or (3) account number or credit card number or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Who has to notify:

- A person or business that conducts business in this state and that owns or licenses computerized data that includes personal information.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

Not specifically addressed.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. Notification is required after the law enforcement agency determines that it will not compromise the investigation.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$250,000 or number of persons exceeds 500,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting and (iii) notice to major territory-wide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if a technical breach does not seem reasonably likely to subject individuals to a risk of criminal activity.

EXISTING POLICY:

- Certain notice requirements may be satisfied if a person or business maintains its own notification procedures consistent with the timing requirements of state law; and if the person or business notifies affected individuals in accordance with its policies.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business when the personal information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information that is lawfully made available to the general public from federal, state, or local government records.

ENCRYPTION:

- Notice is not required if the information is encrypted.

STATUTE CITATION

Wash. Code Ann. § 19.255.010

Original bill text:

<http://apps.leg.wa.gov/documents/billdocs/2005-06/Pdf/Bills/Senate%20Passed%20Legislature/6043-S.PL.pdf>

Statutory code:

<http://apps.leg.wa.gov/RCW/default.aspx?cite=19.255.010>

ATTORNEY GENERAL

Rob McKenna, Esquire
Attorney General of Washington
1125 Washington Street, S.E.
P.O. Box 40100
Olympia, WA 98504-0100
360-753-6200

FBI

Seattle
1110 Third Avenue
Seattle, Washington 98101-2904
<http://seattle.fbi.gov>
206-622-0460
E-mail: Seattle.fbi@ic.fbi.gov

SECRET SERVICE

Seattle
206-553-1922
Spokane
509-353-2532
Electronic Crimes Task Force
Seattle
206-553-1922
Email: seaecwg@einformation.usss.gov

SUMMARY OF LAW - EFFECTIVE DATE - 6/6/08

What is a breach:

Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of this state.

When is notice required:

- Computerized data containing personal information: unencrypted or unredacted
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or identification card number issued in lieu of a drivers license; or (3) financial account number or credit card number or debit card number, in combination with any required security code, access code, or password that would permit access to a financial account.

Who has to notify:

- An individual or entity that maintains personal information as part of a database of personal information regarding multiple individuals.

Who has to be notified:

- The individual.
- The owner or licensee of the information.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice at one time.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

- To the extent possible, a description of info that was reasonably believed to have been accessed or acquired by an unauthorized person, including Social Security numbers, driver's licenses or state identification numbers and financial data.
- A telephone number or website to contact the entity to learn: (A) what types of info the entity maintained about individuals; and (B) whether or not the entity maintained info about that individual.
- The toll-free contact telephone numbers and addresses for the major credit reporting agencies and info on how to place a fraud alert or security freeze.

Timing of notice:

- Without unreasonable delay.
- Notification may be delayed if a law enforcement agency determines and advises the individual/entity that it will impede a criminal or civil investigation or jeopardize homeland or national security. Notification is required after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize homeland or national security.
- Notification may be delayed to determine the scope of the breach and restore the reasonable integrity of the system.

Permitted delivery of notice:

- Written to the postal address in the individual's/entity's records.
- Telephonic.
- Electronic, if electronic notice is consistent with E-Sign requirements.
- Substitute notice may be done if cost of providing notice exceeds \$50,000 or number of persons exceeds 100,000 or sufficient contact information not available. All of the following must be done: (i) email; (ii) web site posting and (iii) notice to major territory-wide media.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if it is reasonably believed that the breach has not caused or will not cause identity theft or other fraud.

STATUTORY:

- Notice is not required to credit reporting agencies if subject to the Gramm-Leach-Bliley Act (GLB).
- Entities are deemed to be in compliance with some or all of the state statute's requirements if they act in accordance with the notification guidelines prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.
- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are in compliance with the notification requirements or procedures pursuant to the rules, regulation, procedures or guidelines established by the primary or functional regulator.

EXISTING POLICY:

- Certain notice requirements may be satisfied if an entity maintains its own notification procedures consistent with the timing requirements of state law; and if the entity notifies affected individuals in accordance with its procedures.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

ENCRYPTION:

- Notice is not required if the information is encrypted.

STATUTE CITATION

W. Va. Code § 46A-2A-101 through § 46A-2A-105

Original bill text:

<http://www.legis.state.wv.us/Bill>

[Text_HTML/2008_SESSIONS/RS/Bills/SB340%20SUB1.htm](http://www.legis.state.wv.us/Bills/SB340%20SUB1.htm)

Statutory code:

<http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=46a&art=2A#2A>

ATTORNEY GENERAL

Darrell V. McGraw, Jr., Esquire
Attorney General of West Virginia
West Virginia State Capitol Building 1
Room 26-E
Charleston, WV 25305
304-558-2021

FBI

Pittsburgh, PA **FBI field office Pittsburgh, PA also covers West Virginia*
3311 East Carson St.
Pittsburgh, Pennsylvania 15203
<http://pittsburgh.fbi.gov>
(412) 432-4000

SECRET SERVICE

Charleston
304-347-5188

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 3/31/06

What is a breach:

If any entity whose principal place of business is located in this state or an entity that stores personal information in this state knows that personal information in the entity's possession has been obtained by a person whom the entity has not authorized to obtain the personal information, the entity shall make reasonable efforts to notify each individual who is the subject of the personal information.

When is notice required:

- Computerized data containing personal information: unencrypted, unredacted or unaltered in a manner that renders the data unreadable.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or identification number; (3) financial account number including a credit or debit card number, or any required security code, access code, or password that would permit access to a individual's financial account; (4) DNA profile; or (5) unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

Who has to notify:

- An entity whose principal place of business is located in this state or an entity that stores personal information in this state.
- A person storing personal information shall notify the owner or licensee.

Who has to be notified:

- The individual.
- The nationwide credit reporting agencies must be notified if more than 1,000 individuals receive notice of a single incident.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

- The notice shall indicate that the entity knows of the unauthorized use of personal information pertaining to the individual.

Timing of notice:

- Within a reasonable time not to exceed 45 days.
- Notification may be delayed if a law enforcement agency, in order to protect an investigation or homeland security, asks an entity not to provide a notice that is otherwise required for any period of time. Notification is required at the end of that time period.

Permitted delivery of notice:

- Written.
- A method the entity has previously employed to communicate with the subject of the personal information.
- A method reasonably calculated to provide actual notice to the subject of the personal information, if an entity cannot with reasonable diligence determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if the acquisition of personal information does not create a material risk of identity theft or fraud.

STATUTORY:

- Exemptions from certain requirements for entities subject to, and in compliance with, the privacy and security requirements of Title V of the Gramm-Leach-Bliley Act (GLB) or their contractors if they have a breach policy in effect.
- Exemptions from certain requirements for covered entities in compliance with Health Insurance Portability and Accountability Act (HIPAA).

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition by an employee or agent of the entity, if the personal information is used for a lawful purpose of the entity.

PUBLIC RECORDS:

- Notice is not required if the information consists of publicly available information, meaning any information that an entity reasonably believes is one of the following:
 - Lawfully made widely available through any media.
 - Lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law.

ENCRYPTION:

- Notice is not required if the information is encrypted.

STATUTE CITATION

Wis. Statutes Ann. § 895.507

Original bill text:

<http://www.legis.state.wi.us/2005/data/SB-164.pdf>

Statutory code:

<http://www.legis.state.wi.us/statutes/2005/05Stat0895.pdf>

ATTORNEY GENERAL

J. B. Van Hollen, Esquire
Attorney General of Wisconsin
State Capitol Suite 114 E.
P.O Box 7857
Madison WI, 53707-7857
608-266-1221

FBI

Milwaukee
330 East Kilbourn Avenue
Suite 600
Milwaukee, Wisconsin 53202-6627
<http://milwaukee.fbi.gov>
414-276-4684
E-mail: Milwaukee@ic.fbi.gov

SECRET SERVICE

Madison
608-264-5191

Milwaukee
414-297-3587

CONSUMER CREDIT REPORTING AGENCIES CONTACT INFORMATION:

Experian®: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.

Equifax®: Send an e-mail to businessrecordsecurity@equifax.com.

TransUnion®: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

SUMMARY OF LAW - EFFECTIVE DATE - 7/1/07

What is a breach:

Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident.

When is notice required:

- Computerized data containing personal information: unredacted.
- Personal information: First name or first initial and last name in combination with (1) Social Security number; (2) drivers license number or identification card number; (3) account number or credit card number or debit card number, in combination with any required security code, access code, or password that would permit access to a individual's financial account; (4) tribal identification card; or (5) Federal or state government issued identification card.

Who has to notify:

- A person or business.
- A person who maintains the data shall notify the business entity on whose behalf the data is maintained. The person and the business entity may agree which will provide any required notice, provided only a single notice for each breach shall be required. If an agreement regarding notification cannot be reached, the person who has the direct business relationship with the state resident shall provide the notice.

Who has to be notified:

- The individual.
- Regulatory/law enforcement notice not specifically addressed.

Required contents of notice:

- A toll-free number that the individual may use to contact the person collecting the data, or his agent; and from which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies.

Timing of notice:

- The most expedient time possible and without unreasonable delay.
- Notification may be delayed if a law enforcement agency notifies in writing that it may seriously impede a criminal investigation.
- Notification may be delayed to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Permitted delivery of notice:

- Written.
- Electronic.
- Substitute notice may be done (1) if the cost of providing notice exceeds \$10,000 for Wyoming-based persons or businesses and \$250,000 for all other businesses operating but not based in Wyoming; or (2) if the affected class of subject persons to be notified exceeds 10,000 for Wyoming-based persons or businesses and 500,000 for all other businesses operating but not based in Wyoming; or sufficient contact information not available. All of the following must be done: (i) web site posting and (ii) notice to major territory-wide media (notice to media shall include a toll-free phone number where an individual can learn whether or not that individual's personal data is included in the security breach).

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if, in good faith after a reasonable and prompt investigation, it is determined that the misuse of personal identifying information has not occurred or is not reasonably likely to occur.

STATUTORY:

- Entities are deemed to be in compliance with some or all of the state statute's requirements if they are subject to the Gramm-Leach-Bliley Act (GLB) and notice is in compliance with the applicable legal requirements.

GOOD FAITH:

- Notice is not required if there has been a good faith acquisition of personal identifying information by an employee or agent of a person or business for the purposes of the person or business is not a breach, provided that the personal identifying information is not used or subject to further unauthorized disclosure.

PUBLIC RECORDS:

- Notice is not required if the information consists of information, regardless of its source, contained in any federal, state or local government records or in widely distributed media that are lawfully made available to the general public.

ENCRYPTION:

- Notice is not required if the information is encrypted.

STATUTE CITATION

Wyo. Stat. § 40-12-501 through § 40-12-502

Original bill text:

<http://legisweb.state.wy.us/2007/Enroll/SF0053.pdf>

Statutory code:

<http://legisweb.state.wy.us/statutes/statutes.aspx?file=titles/Title40/Title40.htm>

ATTORNEY GENERAL

Greg Phillips, Esquire
Attorney General of Wyoming
123 State Capitol Building
200 W. 24th Street
Cheyenne, WY 82002
307-777-7841

FBI

Denver, CO * *FBI field Office Denver, CO covers surrounding areas including Wyoming*
8000 East 36th Avenue
Denver, Colorado 80238
<http://denver.fbi.gov>
303-629-7171

Salt Lake City, UT * *FBI field office Salt Lake City, UT also covers Yellowstone National Park within Wyoming*
257 East 200 South
Suite 1200
Salt Lake City, Utah 84111-2048
<http://saltlakecity.fbi.gov>
801-579-1400
E-mail: SaltLakeCity@ic.fbi.gov

SECRET SERVICE

Cheyenne
307-772-2380

SUMMARY OF MEMO DATED 5/22/07 REQUIRING AGENCY ACTION BY 9/19/07

What is a breach:

Loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for any other authorized purpose have access or potential access to personally identifiable information, whether physical (paper documents) or electronic.

When is notice required:

- Personally identifiable information: information which can be used to distinguish or trace an individual's identity, such as: (1) name; (2) Social Security number; or (3) biometric records, etc.; alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as: (1) date and place of birth, or (2) mother's maiden name, etc.

Who has to notify:

- Federal executive departments and agencies.

Who has to be notified:

- US-CERT;
- The issuing bank if the breach involves government-authorized credit cards;
- To those individuals and/or third parties affected by the breach;
- Persons and entities in a position to cooperate, either by assisting in notification or preventing or minimizing harms;
- The public media;
- The Federal information security incident center;
- Law enforcement agencies and Inspectors General;
- An office designated by the President for any incident involving a national security system;
- Any other agency or office in accordance with law or as directed by the President.

Required contents of notice:

The notification should be in writing with concise, conspicuous, plain language and include:

- A brief description, including the date(s) of the breach and of its discovery.
- To the extent possible, a description of the personal information involved (name, Social Security number, date of birth, home address, and account number).
- Whether the info was encrypted or protected by other means, if such info would not further compromise the system security.
- What protective steps to take against potential harm, if any.
- What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against future breaches.
- Who affected individuals should contact at the agency for more info (toll-free telephone number, e-mail and postal address).

Timing of notice:

- Without unreasonable delay following the discovery of a breach.
- Notification may be delayed for law enforcement or national security considerations if it would seriously impede the investigation of the breach or the affected individuals. However, any delay should not exacerbate risk or harm to any affected individuals.
- Notification may be delayed to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized data system compromised.

Permitted delivery of notice:

The following types of notice may be considered:

- Mail, front of the envelope should alert recipients, e.g., “Data Breach Information Enclosed”, and should be marked with the agency name.
- Telephonic, if urgency dictates immediate and personalized notice and/or when a limited number of individuals are affected, but should be contemporaneous with written notice by first-class mail.
- E-mail, if individual has provided an e-mail address and has expressly consented to e-mail as the primary means of communication and no known mailing address is available.
- Substitute notice may be done if sufficient contact information not available. All of the following must be done: (i) substitute notice should consist of conspicuous posting on the agency home page; and (ii) notification to major print and broadcast media, including major media in areas where the affected individuals reside (notice to media should include a toll-free phone number where an individual can learn if his/her personal information is included in the breach).

Agencies should post information and notification in a clearly identifiable location on the agency home page as soon as possible after discovery and the decision to provide notification.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

Agencies should exercise care to evaluate the benefit of notifying the public of low impact incidents. Agencies should consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach. Five factors should be considered to assess the likely risk of harm:

- Nature of the data elements breached
- Number of individuals affected
- Likelihood the information is accessible and usable
- Likelihood the breach may lead to harm
- Ability of the agency to mitigate the risk of harm

ENCRYPTION:

- Notice may not be necessary if the information is properly encrypted because the information would be unusable.

STATUTE CITATION

OMB Memorandum M-07-16: Safeguarding Against and Responding to the Breach of Personal Identifiable Information

<http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>

INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE

SUMMARY

What is a breach:

Unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.

When is notice required:

- Any record containing nonpublic personal information about a customer, whether in paper, electronic, or other form.
- Sensitive customer information: Name, address, or telephone number, in combination with (1) Social Security number, (2) drivers license number, (3) account number, (4) credit card number or debit card number, or (5) a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

Who has to notify:

- Financial institutions subject to the jurisdiction of the Comptroller at the Treasury Department, Federal Reserve, Federal Deposit Insurance Corporation (FDIC), or Office of Thrift Supervision.
- Service providers contracted to notify the financial institution's customers or regulator on its behalf.

Who has to be notified:

- Primary federal regulator as soon as possible.
- Appropriate law enforcement authorities.
- Customers, when warranted.
- Financial institutions are encouraged to notify the nationwide consumer reporting agencies prior to sending notices to a large number of customers that include contact information for the reporting agencies.

Required contents of notice:

In a clear and conspicuous manner, the notice should include:

- A description of the incident in general terms.
- Type of customer information that was the subject of unauthorized access or use.
- A general description of what the institution has done to protect the customers' information from further unauthorized access.
- A telephone number that customers can call for further information and assistance.
- A reminder to customers of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the financial institution.

The notice should include the following additional items, when appropriate:

- A recommendation that the customer review account statements and immediately report any suspicious activity to the institution;
- A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;
- A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE

(CONTINUED)

- An explanation of how the customer may obtain a credit report free of charge; and
- Information about the availability of the Federal Trade Commission's (FTC) online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the FTC, and should provide the FTC's web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.

Timing of notice:

- As soon as possible following a reasonable investigation conducted to promptly determine the likelihood that misuse of the information about a customer has occurred or is reasonably possible.

Permitted delivery of notice:

- Any manner designed to ensure that a customer can reasonably be expected to receive notice. For example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if there is no substantial harm or inconvenience that could result.

STATUTE CITATION

Unauthorized Access to Customer Information and Customer Notice

<http://edocket.access.gpo.gov/2005/pdf/05-5980.pdf>

FTC HEALTH BREACH NOTIFICATION RULE

SUMMARY OF LAW - EFFECTIVE DATE - 9/24/09

What is a breach:

With respect to unsecured Personal Health Records (PHR) identifiable health information, acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of information.

When is notice required:

- Following the discovery of a breach of security of unsecured PHR identifiable health information that is in a personal health record maintained or offered by such vendor, and each PHR related entity.
- Personal Health Record (PHR) is information that (i) is provided by or on behalf of the individual; (ii) identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Who has to notify:

- Vendor of personal health records.
- PHR related entity.
- Third party service provider.

Who has to be notified:

- The individual U.S. citizen or resident.
- The individual's next of kin if the individual is deceased and if the individual had provided contact information and authorization.
- The FTC.
- If 500 or more residents of a State or jurisdiction, notice shall be provided to prominent media outlets serving the State or jurisdiction.

Required contents of notice:

Plain language and to the extent possible:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PHR identifiable health information that were involved in the breach;
- Steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the entity that suffered the breach is doing to investigate the breach, to mitigate harm, and to protect against any further breaches;
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address.

For substitute notice in media or web posting, a toll-free number, which shall remain active for at least 90 days where an individual can learn whether or not the individual's secured PHR identifiable health information was included.

Timing of notice:

- Without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. A breach of security shall be treated as discovered as of the first day on which such breach is known or reasonably should have been known to the vendor of personal health records, PHR related entity, or third party service provider, respectively.
- If a law enforcement official determines that a notification, notice, or posting required would impede a criminal investigation or cause damage to national security, such shall be delayed.
- If 500 or more individuals, then notice to the FTC shall be provided as soon as possible and in no case later than 10 business days following discovery.
- If less than 500 individuals, a log of any such breaches may be submitted annually no later than 60 calendar days following the end of the calendar year.

Permitted delivery of notice:

Individual Notice

- Written (by first class mail at last known address).
- Email (if individual is given clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise that choice).
- Substitute notice if the contact information for 10 or more individuals is insufficient or out-of-date in a form reasonably calculated to reach the individuals affected through: (i) a conspicuous posting for 90 days on the home page; or (ii) major print or broadcast media, including major media in geographic areas where the individuals affected likely reside.
- Telephone or other means, as appropriate, in any case deemed by the vendor or PHR related entity to require urgency because of possible imminent misuse.

WHEN IS NOTICE NOT REQUIRED

STATUTORY:

- Notice is not required from a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity.

ENCRYPTION:

- Notice is not required if the PHR identifiable information is secured, meaning protected through the use of technology or methodology specified by HHS guidance in § 13402(h)(2) of the American Reinvestment and Recovery Act (see above).

STATUTE CITATION

16 C.F.R. Part 318

<http://www.ftc.gov/os/2009/08/R911002hbn.pdf>

<http://www.ftc.gov/os/2009/08/R911002hbnform.pdf>

HHS BREACH NOTIFICATION FOR UNSECURED HEALTH INFORMATION

SUMMARY OF LAW - EFFECTIVE DATE - 9/23/09

What is a breach:

- Acquisition, access, use, or disclosure of protected health information in a manner not permitted which compromises the security or privacy of the protected health information.

When is notice required:

- Following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.
- A breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

Who has to notify:

- The covered entity.
- A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach, including to the extent possible, the identification of each individual and any other available information that the covered entity is required to include in notification to the individual.

Who has to be notified:

- Each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.
- For a breach involving more than 500 residents of a State or jurisdiction, a covered entity shall notify prominent media outlets serving the State or jurisdiction without unreasonable delay and in no case later than 60 calendar days after discovery of a breach (same content requirement as for consumers).
- The HHS Secretary: For breaches of 500 or more, contemporaneously with the consumer notice; For breaches of less than 500, maintain a log or other documentation for not later than 60 days after the end of each calendar year.

Required contents of notice:

To the extent possible, the notice shall be written in plain language and include:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

HHS BREACH NOTIFICATION FOR UNSECURED HEALTH INFORMATION

(CONTINUED)

Timing of notice:

- Without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
- If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

Permitted delivery of notice:

- Written (by first-class mail to the individual at the last known address of the individual or to the next of kin or personal representative of the individual if the covered entity knows the individual is deceased and has the address).
- Email (if the individual agrees to electronic notice and such agreement has not been withdrawn).
- The notification may be provided in one or more mailings as information is available.
- Substitute notice (if there is insufficient or out-of-date contact information that precludes written notification, a substitute form of notice reasonably calculated to reach the individual shall be provided). In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.
- In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate.

HHS BREACH NOTIFICATION FOR UNSECURED HEALTH INFORMATION

(CONTINUED)

WHEN IS NOTICE NOT REQUIRED

HARM TRIGGER:

- Notice is not required if there is no significant risk of financial, reputational, or other harm to the individual.

GOOD FAITH:

- Notice is not required if there is (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted. (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted. (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

ENCRYPTION:

- Notice is not required if the protected health information is rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology.

STATUTE CITATION

45 CFR Parts 160 and 164

<http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>

ADDITIONAL LAW ENFORCEMENT CONTACTS*

NATIONAL

FBI HEADQUARTERS

J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001
(202) 324-3000
<http://www.fbi.gov/>

SECRET SERVICE HEADQUARTERS

245 Murray Drive
Building 410
Washington, DC 20223
(202) 406-8000
<http://www.secretservice.gov/>

U.S. ATTORNEY GENERAL

Eric Holder, Esquire
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001
(202) 514-2000
<http://www.usdoj.gov/ag/>

FEDERAL TRADE COMMISSION HEADQUARTERS

600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

ALABAMA

FBI
Mobile
200 N. Royal Street
Mobile, Alabama 36602
<http://mobile.fbi.gov>
(251) 438-3674

Birmingham
1000 18th Street North
Birmingham, Alabama 35203
<http://birmingham.fbi.gov>
(205) 326-6166

Electronic Crimes Task Force
Birmingham
(205) 731-1144
Email: bhmecw@information.usss.gov

SECRET SERVICE

Mobile
(251) 441-5851
Montgomery
(334) 223-7601

ATTORNEY GENERAL

Luther Strange
Office of the Attorney General
P.O. Box 300152
Montgomery, AL 36130-0152
334-242-7300

KENTUCKY

FBI
Louisville
12401 Sycamore Station Pl.
Louisville, Kentucky 40299-6198
<http://louisville.fbi.gov>
Louisville.LS@ic.fbi.gov
(502) 263-6000

SECRET SERVICE

Lexington
(859) 223-2358

Electronic Crimes Task Force
Louisville
(502) 582-5171
Email: louecwg@information.usss.gov

ATTORNEY GENERAL

Jack Conway, Esquire
Attorney General of Kentucky
700 Capitol Avenue
Capitol Building, Suite 118
Frankfort, KY 40601
(502) 696-5300

NEW MEXICO

FBI
Albuquerque
4200 Luecking Park Ave. NE
Albuquerque, New Mexico 87107
<http://albuquerque.fbi.gov>
(505) 889-1300
E-mail: AQ.FBI@ic.fbi.gov

SECRET SERVICE

Albuquerque
(505) 248-5290

ATTORNEY GENERAL

Gary King, Esquire
Attorney General of New Mexico
P.O. Drawer 1508
Sante Fe, NM 87504
505-827-6000

SOUTH DAKOTA

FBI
Minneapolis * *FBI field office Minneapolis, MN also covers South Dakota*
111 Washington Avenue South
Suite 1100
Minneapolis, Minnesota 55401-2176
<http://minneapolis.fbi.gov>
(612) 376-3200

SECRET SERVICE

Sioux Falls
(605) 330-4565

ATTORNEY GENERAL

Marty J. Jackley, Esquire
Attorney General of South Dakota
1302 East Highway 14
Suite 1
Pierre, SD 57501-8501
(605) 773-3215

AMERICAN SAMOA

FBI
Honolulu
Prince Kuhio FOB
300 Ala Moana Boulevard
Room 4-230
Honolulu, Hawaii 96813
<http://honolulu.fbi.gov>
(808) 566-4300

American Samoa Resident Agency
Pago Plaza, Suite 217
Post Office Box 6544
Pago Pago, American Samoa 96799
(684) 633-1313

ATTORNEY GENERAL

Fepulea'i A. Ripley, Jr., Esquire
Attorney General of American Samoa
American Samoa Government
Executive Office Building
Utulei, Territory of American Samoa
Pago Pago, AS 96799
(684) 633-4163

GUAM

FBI
Honolulu * *FBI field Office Honolulu, HI covers surrounding area including Guam*
Prince Kuhio FOB
300 Ala Moana Boulevard
Suite 4-230
Honolulu, Hawaii 96813
<http://honolulu.fbi.gov>
(808) 566-4300

Guam Resident Agency *
First Hawaiian Bank Building,
Maite Branch
400 Route 8, Suite 402
Maite, Guam 96910
671) 472-7465

SECRET SERVICE

Hagatna
(671) 472-7395

ATTORNEY GENERAL

Lenny Rapadas, Esquire
Attorney General of Guam
287 West O'Brien Drive
Hagatna, Guam 96910
671-475-3324
law@guamattorneygeneral.com

NORTHERN MARIANA ISLANDS

FBI
Honolulu
Prince Kuhio FOB
300 Ala Moana Boulevard
Room 4-230
Honolulu, Hawaii 96850-0053
<http://honolulu.fbi.gov>
(808) 566-4300

ATTORNEY GENERAL

Edward T. Buckingham, Esquire
Attorney General of Northern Mariana Islands
Administration Building
P.O. Box 10007
Saipan, MP 96950-8907
(670) 664-2341

*As of January 2012, these states have not passed breach notification regulations.

ABOUT INTERSECTIONS (WWW.INTERSECTIONS.COM)

Intersections Inc. ([Nasdaq: INTX](#)) is a leading provider of consumer and corporate identity risk management services. Intersections provides various levels of service to more than 9.6 million consumers. Those services are offered through North America's leading financial institutions, directly to consumers under Intersections' award-winning IDENTITY GUARD(R) brand (<http://www.identityguard.com>), and through the company's exclusive partnership with [ITAC](#), the Identity Theft Assistance Center. Since 1996, Intersections has protected the identities of more than 34 million consumers.

Through our exclusive partnership with ITAC, the Identity Theft Assistance Center – a member-supported, non-profit organization founded in 2004 by the Financial Services Roundtable with unique operational ties to fraud prevention departments at major financial institutions – we can directly help resolve your customers' identity theft problems. No other data breach response provider can provide this level of victim assistance.

Call us at [877.983.9850](tel:877.983.9850) or email us at Partner@intersections.com to find out how we can help your company establish a Breach ReadinessSM program.

If you have currently experienced a data breach, call us at [888.283.1725](tel:888.283.1725) or email us at DataBreachServices@Intersections.com.





Intersections, Inc.
3901 Stonecroft Boulevard
Chantilly, VA 20151
Toll-free: 1.888.283.1725
DataBreachServices@Intersections.com
www.Intersections.com