CONTRACTS
The Upside of Risk

THE DEVIL'S IN THE DETAILS:

HOW THE STATE OF NOTICE OF BREACH PROVISIONS IMPACT THIRD-PARTY RISK AND OPERATIONS

Agenda for Notice of Breach

1. Elements
2. Federal Guidance
3. Sample State Law Challenges
4. Best Practices

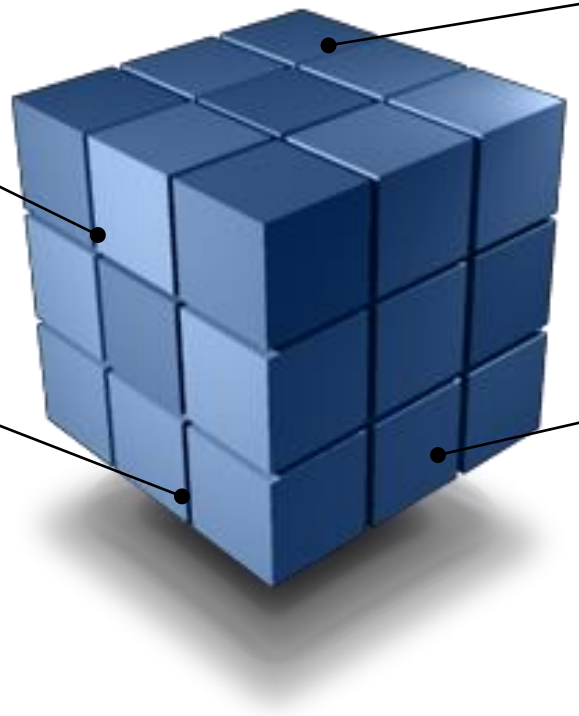
Elements of Notice of Breach Issues

- What data is protected?
- What is a breach?
- When do I have a notify someone of breach?

Federal Guidance on Notice of Breach

OCC Bulletin
2013-29

FDIC
FIL-44-2008



Federal Reserve Board
Guidance 12/4/2013

NCUA
Letter No. 07-CU-13
12/2007;07-01
10/2007

California – Notice of Breach - Data

Data Protected:

General Statute: Cal. Civ. Code §§ 1798.29, 1798.80, 1798.82, and 1798.84

The general statute protects California residents' "personal information," defined as an individual's first name or initial with last name and one or more of the following data elements, if either the name or data element is unencrypted:

- Social Security number.
- Driver's license or California identification card number.
- Account, credit, 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.
- Medical information, defined as any information regarding an individual's: medical history; mental or physical condition; or diagnosis by a health care professional.

Health insurance information, defined as an individual's: health insurance policy number or subscriber identification number; any unique identifier used by a health insurer to identify the individual; any information in an individual's application and claims history, including any appeals records.

- A user name or email address, in combination with a password or security question and answer that would permit access to an online account.
- Information or data collected through an automatic license plate recognition system. Breach notification requirements **also apply to encrypted information**, if an encryption key or security credential that allows an unauthorized party to render the data readable or usable is also compromised. However, the definition specifically excludes information that is lawfully made available to the general public from federal, state, or local government records. (Cal. Civ. Code §§ 1798.29(g), (h), 1798.82(h),(i).)

California – Notice of Breach
Breach Defined

Breach:

General Statute: Cal. Civ. Code §§ 1798.29, 1798.80, 1798.82, and 1798.84 Triggering Events for Notice to Affected Persons
The notification requirement is triggered on discovery of a "breach of the security of the system," which means an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity. However, it excludes good faith acquisition of personal information by the entity's employees and agents for the purposes of the entity if the personal information is not used or subject to further unauthorized exposure. (Cal. Civ. Code §§ 1798.29(f), 1798.82(g).)

Risk Assessment
The notification obligation is not subject to a risk assessment.

Effect of Encryption, Redaction, or Other Means of Making Information Unreadable The statute applies to personal information that is either:
• Not encrypted.
• Encrypted, if an encryption key or security credential that allows an unauthorized party to render the data readable or usable is also compromised.
(Cal. Civ. Code §§ 1798.29(a), 1798.29(g), and 1798.82(h) and see Protected Personal Information).

California – Notice of Breach - Timing

Notice Timing:

General Statute: Cal. Civ. Code §§ 1798.29, 1798.80, 1798.82, and 1798.84

The covered entity must notify affected persons in the **most expedient time possible** and without unreasonable delay, consistent with:

- The legitimate needs of law enforcement.
- Any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

However, if a law enforcement agency determines that providing notice will likely impede a criminal investigation, the covered entity may delay notice until the law enforcement agency determines that doing so will not compromise the investigation. (Cal. Civ. Code §§ 1798.29(a), 1798.29(c), and 1798.82(c).)

Connecticut – Notice of Breach - Data

Data Protected: General Statute: Conn. Gen. Stat. § 36a-701b
The statute protects Connecticut residents' "personal information," defined as an individual's first name or initial with last name combined with one of the following, if the information is unencrypted or not secured by any other method or technology rendering the personal information unreadable or unusable (see Effect of Encryption, Redaction, or Other Means of Making Information Unreadable):
• Social Security number; • Driver's license or state identification card number; • Account, credit card, or debit card number, in combination with any security code, access code, or password required to access the account.
Personal information does not include publicly available information that is lawfully made available to the general public from either: • Federal, state, or local government records. • Widely distributed media.
(Conn. Gen. Stat. Ann. § 36a-701b(a).)
Health Insurer Statute: Conn. Gen. Stat. Ann. § 38a-999b
The statute protects Connecticut residents' "personal information," defined as an individual's first name
or first initial with last name in combination with any one or more of the following data elements:
• Social Security number.• Driver's license or state identification number. • Protected health information as defined in 45 CFR 160.103.• Taxpayer identification number.• Alien registration number.• Government passport number.• Demand deposit account number.• Savings account number. • Credit or debit card number. • Unique biometric data such as a fingerprint, a voice print, a retina, or an iris image or other unique physical representations.

Effect of Encryption, Redaction, or Other Means of Making Information Unreadable
The statutes only applies to unencrypted or otherwise readable electronic files, media, databases, or computerized data (Conn. Gen. Stat. Ann. § 36a-701b(a); § 38a-999b(e)(1), and see Protected Personal Information).

Connecticut – Notice of Breach
Breach Defined

Breach:

General Statute: Conn Gen Stat § 36a-701b and Health Entities Statute: Conn. Gen. Stat. Ann. § 38a-999b

Triggering Events for Notice to Affected Persons

The statutes' notification obligations are triggered when a covered entity discovers a "breach of security," defined as the unauthorized access to or acquisition of unencrypted electronic files, media, databases, or computerized data containing personal information (Conn. Gen. Stat. Ann. § 36a-701b(a)).

Risk Assessment
Notice is not required if the covered entity determines there will likely be no harm to the affected individuals after an investigation and consultation with relevant federal, state, and local agencies responsible for law enforcement (Conn. Gen. Stat. Ann. § 36a-701b(b); § 38a-999b(e)(1)).

Connecticut – Notice of Breach - Timing

Notice Timing:

General Statute: Conn Gen Stat § 36a-701b and Health Entities Statute: Conn. Gen. Stat. Ann. § 38a-999b
The covered entity must give notice to affected persons **without unreasonable delay, and within 90 days of discovery of the breach**, unless federal law requires sooner notification. Notice may be delayed either:

As necessary to:
- determine the nature and scope of the breach;
- identify the affected individuals; or
- restore the integrity of the data system.
- If a law enforcement agency determines that providing notice will impede a criminal investigation, until the law enforcement agency notifies the covered entity that notification will not compromise the investigation.

(Conn. Gen. Stat. Ann. § 36a-701b(b); § 38a-999b(e)(1).)

Florida – Notice of Breach - Data

Data Protected:

An individual's first name or initial and last name in combination with one or more of the following data elements:

- Social Security number;
- driver's license number, identification card number, passport number, military identification number, or other governmental identification number;
- financial account, 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;
- medical information; or health insurance policy number or health insurance identification number and any unique identifier used by a health insurer to identify an individual.
- **User name or email address, in combination with a password or security question and answer that would permit access to an online account.** (§ 501.171(1)(g)(1), Fla. Stat.)

The definition specifically excludes information about an individual that:

• Has been made publicly available by a federal, state, or local governmental entity.

• Is encrypted or otherwise secured so that it is unreadable (see Effect of Encryption, Redaction or Other Means of Making Information Unreadable). (§ 501.171(1)(g)(2), Fla. Stat.)

Effect of Encryption, Redaction, or Other Means of Making Information Unreadable

The statute does not apply to encrypted, secured, or de-identified information (§ 501.171(1)(g)(2), Fla. Stat. and see Protected Personal Information).

Florida – Notice of Breach
Breach Defined

Breach:

The statute's notification obligations are triggered on a covered entity's determination that there was a "breach of the security of the system," meaning unauthorized access to computerized data containing personal information. Good faith acquisition by an employee or agent of the covered entity is not a breach if the information is not used or subject to further unauthorized disclosure. (§ 501.171(1)(a), Fla. Stat.)

Risk Assessment

Notice is not required if the covered entity reasonably determines that the breach has not and is not likely to result in identity theft or any other financial harm to the persons whose personal information has been acquired and accessed after:

- An appropriate investigation.
- Consultation with relevant federal, state, and local agencies responsible for law enforcement.

The covered entity must:

- Document its determination in writing.
- Maintain the documentation for five years.
- Provide the determination to the Department of Legal Affairs within 30 days.

(§ 501.171(4)(c), Fla. Stat.)

Florida – Notice of Breach - Timing

Notice Timing:

The covered entity must give notice to affected persons without unreasonable delay, but no later than 30 days after determining the breach, consistent with:

- The legitimate needs of law enforcement.
- Measures necessary to:
- determine the scope of the breach;
- identify affected individuals; and
- restore the reasonable integrity of the system.

(§ 501.171(4)(a), Fla. Stat.)

Notification to individuals may be delayed if law enforcement determines that notification would interfere with a criminal investigation and requests a delay in writing (§ 501.171(4)(b), Fla. Stat.).

Kansas – Notice of Breach - Data

Data Protected:

The statute protects Kansas residents' "personal information," defined as an individual's first name or initial with last name linked to one or more of the following data elements, if the data elements are unencrypted and unredacted:

- Social security number.
- Driver's license or state ID card number.
- Financial account, credit card or debit card number, alone or in combination with any security code, access code, or password required to access the account.

However, the definition specifically excludes publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Kan. Stat. Ann. §§ 50-7a01(g), (h).)

Effect of Encryption, Redaction, or Other Means of Making Information Unreadable

The Kansas statute only applies to information that is unencrypted or unredacted (Kan. Stat. Ann. § 50-7a01(g) and see Protected Personal Information).

Kansas – Notice of Breach
Breach Defined

Breach:

Triggering Events for Notice to Affected Persons
The notification obligation is triggered when the entity learns of a "security breach," meaning the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity that causes, or that the individual or entity reasonably believes has caused or will cause, identity theft to any consumer. However, it excludes good faith acquisition of personal information by the covered entity's employees and agents for the entity's legitimate purposes
if the personal information is not improperly used or is not subject to further unauthorized disclosure
(Kan. Stat. Ann. § 50-7a01(h)).

Risk Assessment
Notification is required only if after a prompt, good faith, and reasonable investigation, the covered entity determines that personal information has been or is reasonably likely to be misused (Kan. Stat. Ann. § 50-7a02(a)).

Kansas – Notice of Breach - Timing

Notice Timing:

The covered entity must give notice to affected persons in the **most expedient time possible** and without unreasonable delay, consistent with:

- The legitimate needs of law enforcement.
- Any measures necessary to:
- determine the scope of the breach; and
- restore the reasonable integrity of the computerized data system.

(Kan. Stat. Ann. § 50-7a02(a).)

If a law enforcement agency determines that providing notice will impede a criminal investigation, the covered entity may delay notice until the law enforcement agency determines notification will no longer impede the investigation (Kan. Stat. Ann. § 50-7a02(c)).

Minnesota – Notice of Breach - Data

Data Protected:

The statute protects Minnesota residents' "personal information," defined as an individual's first name or initial with last name and one or more of the following data elements, if the data element is unencrypted or not secured by another method of technology that makes electronic data unreadable or unusable, or secured but the encryption key, password, or other means necessary for reading or using the data was also acquired:

- Social Security number.
- Driver's license or state identification card number.
- Account, credit, or debit card number, in combination with any security code, access code, or password required to access the account.

However, the definition specifically excludes publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Minn. Stat. Ann. §§ 325E.61(1)(e), (f).)

Effect of Encryption, Redaction, or Other Means of Making Information Unreadable
The statute only applies to personal information that is not encrypted or otherwise unreadable (Minn. Stat. Ann. § 325E.61(1)(a) and see Protected Personal Information).

Minnesota – Notice of Breach
Breach Defined

Breach:

The statute's notification obligations are triggered on discovery of a "breach of the security of the system," defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. However, it excludes good faith acquisition of personal information by the covered entity's employees and agents for the entity's purposes if the personal information is not used or subject to further unauthorized disclosure. (Minn. Stat. Ann. §§ 325E.61(1)(a), (d).)

Risk Assessment
The notification obligation is not subject to a risk assessment.

Minnesota – Notice of Breach - Timing

Notice Timing:

The covered entity must give notice to affected persons in the **most expedient time possible** and without unreasonable delay, subject to any measures necessary to:

- Determine the scope of the breach.
- Identify the individuals affected.
- Restore the reasonable integrity of the data system.

(Minn. Stat. Ann. § 325E.61(1)(a).)

If a law enforcement agency determines that providing notice will impede a criminal investigation, the covered entity may delay notice (Minn. Stat. Ann. § 325E.61(1)(c)).

Tennessee – Notice of Breach - Data

Data Protected:

The statute protects Tennessee residents' "personal information," defined as an individual's first name or initial with last name and one or more of the following data elements, if either the name or the data element is unencrypted (see Effect of Encryption, Redaction, or Other Means of Making Information Unreadable):

- Social Security number.
- Driver's license or identification card number.
- Account, 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.

However, the definition specifically excludes publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(Tenn. Code Ann. § 47-18-2107(a)(3).)

Under amendments effective April 4, 2017, the statute removes the caveat that limited personal information to instances where the name or data element was unencrypted. It also excludes the following from the definition of personal information:

- **Information that has been encrypted in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2 if the encryption key has not been acquired by an unauthorized person.**
- **Information that has been redacted or otherwise made unusable.**

(H.B. 545, § (1)(a)(4)(B).)

Tennessee – Notice of Breach
Breach Defined

Breach:

Triggering Events for Notice to Affected Persons
The statute's notification obligations are triggered by a covered entity's discovery or notification of a "breach of the security of the system," defined as unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder (Tenn. Code Ann. § 47-18-2107(a)(1)). For the purposes of determining whether a breach has occurred, the statute defines an unauthorized person to include an information holder's employee who acquires personal information and intentionally misuses it for an unlawful purpose (Tenn. Code Ann. § 47-18-2107(a)(4)). Under amendments effective April 4, 2017, the definition of unauthorized person is clarified to mean an information holder's employee who is discovered by the information holder to have obtained personal information with the intent to use it for an unlawful purpose (H.B. 545, § (1)(a)(5)).

Risk Assessment
Notification is required only if the unauthorized acquisition of computerized data materially compromises the security, confidentiality, or integrity of personal information the information holder maintains (Tenn. Code Ann. § 47-18-2107(a)(1)).

Effect of Encryption, Redaction, or Other Means of Making Information Unreadable Under amendments effective July 1, 2016, the statute removed the word "encrypted" from the definition of a breach requiring notification. However, the statute will continue to define personal information that triggers a breach as information that is not encrypted. (Tenn. Code Ann. § 47-18-2107 and see Protected Personal Information). Under amendments effective April 4, 2017, the statute clarifies that information that is encrypted in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2 is not considered personal information, unless the encryption key has also been acquired by an unauthorized person (H.B. 545, § (1)(a)(4)(B)).

Tennessee – Notice of Breach - Timing

Notice Timing:

A covered entity must immediately disclose the breach, but no later than 45 days from the discovery or notification of the breach (Tenn. Code Ann. §§ 47-18-2107(b), 47-18-2107(c)).

However, if a law enforcement agency determines that providing notice will impede a criminal investigation, the covered entity may delay notice no more than 45 days after the law enforcement agency determines it will not compromise the investigation. (Tenn. Code Ann. § 47-18-2107(d).)

Texas – Notice of Breach - Data

Data Protected:

The statute protects "sensitive personal information," defined as an individual's first name or initial and last name and one or more of the following data elements, if both the name and data elements are unencrypted (see Effect of Encryption, Redaction, or Other Means of Making Information Unreadable):

- Social Security number.
- Driver's license number or identification card number.
- 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.
- Information that identifies an individual and relates to:
- the physical or mental health or condition of the individual;
- the provision of health care to the individual; or
- payment for the provision of health care to the individual.

However, the statute specifically excludes from the definition, publicly available information that is lawfully made available to the public from federal, state, or local government records. (Tex. Bus. & Com. Code Ann. § 521.002.)

Effect of Encryption, Redaction, or Other Means of Making Information Unreadable

The Texas statute only applies to unencrypted sensitive personal information unless the encryption key is also breached (Tex. Bus. & Com. Code Ann. § 521.053(a) and see Protected Personal Information).

Texas – Notice of Breach
Breach Defined

Breach:

Triggering Events for Notice to Affected Persons

The notification obligation is triggered by a covered entity's discovery of a “breach of system security,” defined as unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a covered entity, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner. (Tex. Bus. & Com. Code Ann. § 521.053(a)).

Risk Assessment
The notification obligation is not subject to a risk assessment.

Texas – Notice of Breach - Timing

Notice Timing:

The covered entity should give notice to the affected persons **as quickly as possible** or as necessary to:

- Determine the scope of the breach and restore the reasonable integrity of the data system.
- Comply with a request for delay by law enforcement if it determines that notification would impede a criminal investigation.

(Tex. Bus. & Com. Code Ann. §§ 521.053(b) and 521.053(d)).

Best Practices

1) Identify relevant states
2) Take most stringent definition of data, triggering event and notice provision
3) Incorporate into incident response process
4) Incorporate into vendor management process
   - Contract
   - Performance Review

Vendor Management

- Check to see if vendor's that have access to GLBA data are required to provide notice of breach
  - Does it meet State requirements?
- What State law applies in the agreement?
- Create standard language for all vendors that have access to GLBA data and update agreements

Subscribe to get Free Risk and Vendor Management Content in your Inbox

https://ncontracts.com/blog/

CONTACT INFORMATION

(888) 370-5552

Michael.Carpenter@ncontracts.com

ncontracts.com