Joseph M. Burton Partner
jmburton@duanemorris.com
Duane Morris LLP, San Francisco

A run through the California breach notification weeds

A little more than a month ago on 13 September 2016, California Governor Jerry Brown approved Assembly Bill 2828 and thereby initiated important, and potentially far-reaching changes, to California's landmark data breach notification statute. California passed the nation's first data breach notification statute in 2002. The statute is set forth in two essentially identical sections of the California Civil Code. Civil Code § 1798.29 sets forth the breach notification requirements for California Governmental agencies, while the provisions in Code § 1798.82 describe identical requirements for private businesses and individuals doing business in California. For purposes of clarity and convenience, Joseph M. Burton, Partner at Duane Morris LLP, discusses the requirements applicable to businesses.

The inclusion of an encryption safe harbor was meant to incentivise organisations to encrypt personal information under their control.

image: Frederic Legrand - COMEO / Shutterstock.com

Background

Since its initial passage in 2002, the Breach Notification statute has always contained 'safe harbor' language which limited application of its notification requirements to only personal information which had been compromised in a security breach, and which was not encrypted. Prior to passage of AB 2828, Section 1798.82 (a) had consistently provided that:

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

This implicit endorsement of encryption as a means for protecting sensitive personal information was specifically intended by the legislature to encourage its increased adoption and use by businesses in California. There was, however, at least one impediment to achievement of this objective. While encouraging the encryption of personal information, the statute provided no guidance to businesses regarding what it meant to 'encrypt' information.

In 2015 it was amended to define encryption for the first time. Section 1798.82 (i) (4) provides that: '"encrypted" means [to be] rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology, or methodology generally accepted in the field of information security.'

The official legislative comments to the Bill [AB 964] seeking to amend the statute describe its purpose this way: 'Under current law, if the personal information that was stolen was encrypted, businesses are not required to provide notice. This provision encourages businesses who store personal information to adopt encryption so that if information is stolen that information would be less vulnerable to abuse. However, encryption is not clearly defined in [sic] statute. The bill would clarify the statute by defining "encrypted" [...].'

While this particular amendment addressed a long-standing issue, the September 2016 amendments have added an entirely new class of data that significantly expands the nature and scope of activities which may require breach notification. Though Section 1798.82 retains the statute's original language regarding unencrypted personal information under a renumbered subsection (a) (1), it also creates an entirely new subsection (a) (2) which for the first time requires notification in some circumstances even if the compromised personal information is encrypted. The new Section 1798.82 (a) (2) provides for notification when a person:

'whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable.'

While the original statute intended to encourage greater use of encryption as a means of reducing or eliminating the compromise of personal information, the most recent amendments are driven by the realisation that there are, increasingly, some situations in which merely encrypting information may not be enough to ensure that the information remains confidential. The Senate Rules Committee notes clearly describe the situation intended to be addressed by the new amendments this way:

'The inclusion of an encryption safe harbor was meant to incentivize organizations to encrypt personal information under their control. However, the protections offered by encryption are significantly compromised when encrypted data is acquired along with an encryption key that can be used to decrypt the data.'

Practice challenges

The addition of this new class of data is not a trivial change. In addition to the previous requirements for providing breach notification for incidents involving unencrypted personal information, businesses are also required to provide notification if three additional conditions are met: (1) encrypted personal information is reasonably believed to have been acquired; (2) the encryption key or security credential is reasonably believed to have been acquired; and (3) it is reasonably believed that the encryption key or security credential could make the personal information readable or useable. These requirements raise new issues for practitioners. Here are two:

Encrypted personal information

'Encrypted personal information' is the new class of information introduced with the September amendments. Previously, the statute only applied to unencrypted personal information and only defined unencrypted personal information. The original definition of 'personal information' continues to be found in subsection (h) of the statute. Subsection (h)(1) defines personal information as either '[a]n individuals first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted.'

Under this long-standing provision, if either the name or its associated data elements is unencrypted, the data is defined as personal information under the statute, and is also by definition unencrypted personal information because one (or both) of the components of the data is unencrypted.

However, by using the same definition of 'personal information' for both unencrypted and encrypted data, the amended statute may have created an oxymoron which will in some cases defeat the central objective of the amendments. This is so because if both a name and its related data element are 'encrypted' then this form of encrypted data can never be 'personal information' within the meaning of the statute. As such, even if the other provisions of the statute are satisfied, breach notification would not be legally required (as always, in each case there may well be strong business or reputational concerns which would argue in favour of notification even if there is no legal requirement). When the statute only applied to unencrypted personal information syllogistic anomalies of this nature were not possible.

Keys and credentials

Section 1798.82 (a) also introduces two additional new terms to the breach notification equation: 'encryption key' and 'security credential.' Newly added subsection 1798.82 (k) provides that '[f]or purposes of this section, an "encryption key" or "security credential" is a confidential key or process designed to render data useable, readable, and decipherable.'

Though termed an encryption key, its only relevant function (and that of a security credential as well) under the statute is to decrypt data; that is to render data useable, readable, and decipherable. This will be important to bear in mind when considering whether the unlawful acquisition of a particular encryption key requires notification.

During consideration of the 2016 amendments it was asserted that any information which could be used to 'access or decrypt encrypted personal information contained in a data system' is properly considered an encryption key or security credential under the statute. The final language of the statute while ambiguous on this question appears to be more narrowly drawn. The only forms of information mentioned are a confidential key, or a process.

It is not clear whether a 'security credential' is a 'confidential key,' a 'process,' or both. The same question may be asked regarding an 'encryption key.' Certainly a plausible interpretation is that the term 'confidential key' refers to 'encryption key' and the term 'process' refers to the functioning of a 'security credential.'

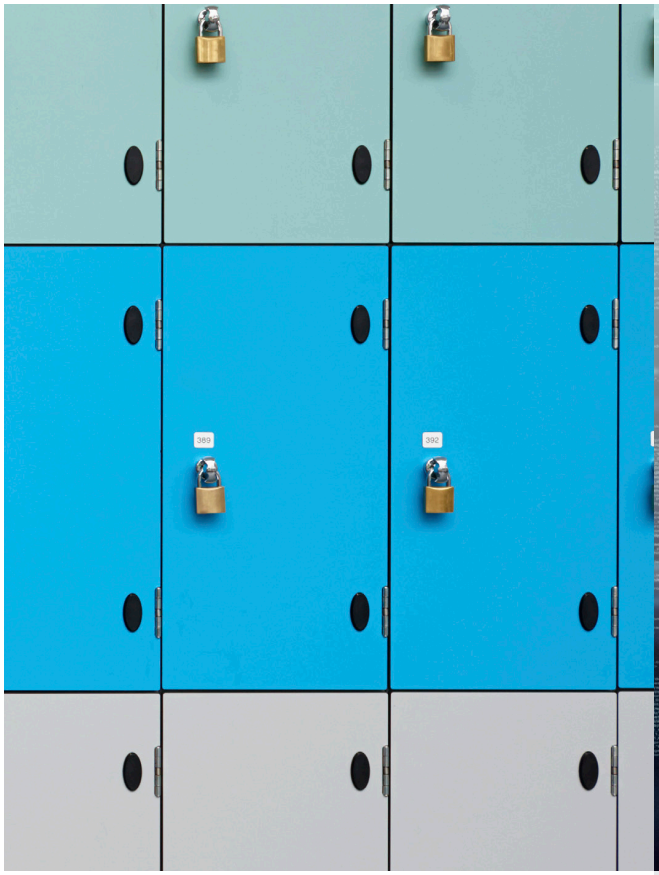
If a 'security credential' is defined as a 'process' does a password, written on a sticky note attached to a stolen encrypted laptop (containing personal information) constitute a security credential? The sticky note is certainly information, but is it a 'process'? Is it a key? If it is either, notification would be legally compelled because both encrypted personal information and a security credential were acquired?

Alternatively, if just the sticky note were stolen, would notification be required?

During the hearings on AB 2828 it was also asserted that the required acquisition of credentials need not be co-incident with the acquisition of the personal information, but may occur at anytime, before or after, the personal information has been acquired. Again, while this position was asserted during the legislative process, the final language of the statute leaves this question open to argument.

However it can be said that the statute does appear to establish a symbiotic relationship between the encrypted personal information and any associated key or credential. Acquisition of both is essential to trigger notification. It therefore appears that the mere acquisition of security credentials need be reported only if at some subsequent time (or even at an earlier time) the associated personal information was acquired.

There are, however, circumstances under which the acquisition of certain security credentials may automatically result in the acquisition of its associated personal information because the credential is itself personal information. Section 1798.82 (h) describes an online security credential which represents an alternative form of 'personal information.' Acquisition of this type of online security credential is therefore both an acquisition of personal information and the acquisition of a security credential. Conversely acquisition of the same type of security credential (account name, password, etc) but which



is not associated with an online account would not constitute personal information and would not require notification unless other associated personal information had been, or is subsequently, also acquired.

The absence of clarity on this issue is of particular interest in light of the increasing number of incidents which involve the theft of security credentials alone (e.g. Yahoo, LinkedIn, etc).

Conclusion

The few issues discussed here make it clear that the new amendments to the California breach notification statute are extremely significant and will undoubtedly impact on the way that businesses evaluate and determine their responses to data breaches. It is therefore important that cyber security practitioners carefully analyse these new provisions.

It is not clear whether a 'security credential' is a 'confidential key,' a 'process,' or both.

G7 publishes cyber security guidelines for financial sector

The Group of Seven industrial powers ('G7') published, on 11 October 2016, its guidelines on Fundamental Elements of Cybersecurity for the Financial Sector ('the Guidelines'). The Guidelines were published following a series of cross-border bank thefts, which continue to threaten 'interconnected global financial systems and the institutions that operate and support those systems.'

In particular, the Guidelines advise financial institutions to 'establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks,' as well as to 'define and facilitate performance of roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the cybersecurity strategy and framework to ensure accountability.' In addition, the Guidelines put emphasis on the necessity of having effective cyber risk and control assessment procedures in place together with the establishment of systematic monitoring processes developed 'to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises.' Finally, the Guidelines outline steps to be taken in the case of a cyber incident and in order to resume operations responsibly.

Further, financial institutions are also advised to share cyber security information with internal and external stakeholders 'on threats, vulnerabilities, incidents, and responses to enhance defenses, limit damage, increase situational awareness, and broaden learning,' as well as to review their cyber security strategies and framework on a regular basis.