EDWARDS WILDMAN

CLIENT ADVISORY

edwardswildman.com

October 2014

An Edwards Wildman Privacy & Data Protection Client Advisory

New California Requirements Shake Up Breach Notification and Data Safeguards

By: Ellen M. Giblin, Mark E.Schreiber, Thomas J. Smedinghoff, Theodore P. Augustinos, Laurie A. Kamaiko and Karen L. Booth

Recent amendments to California statutes governing breach notification and data safeguards impose new obligations by: (1) enhancing breach notification requirements relating to offerings of "identity theft prevention and mitigation services"; (2) expanding the statutory requirement to implement reasonable security measures to protect personal information so that it applies not only to businesses that own or license personal information, but also to third party service providers that maintain such personal information for others; and (3) prohibiting the sale, advertisement for sale, or offer to sell an individual's Social Security number.

The new law regarding the California breach notification requirement related to "identity theft prevention and mitigation services" has already spurred debate on two issues. First, does it *require* the offering of such breach services by entities which sustain a breach of computerized personal information, or does it only apply in cases where such entities decide, in their own discretion, to offer such services? At minimum, the new statute is clear that, if offered, such breach services, must be for at least a year and without charge to the consumer.

Second, what is the scope of the term "identity theft prevention and mitigation services?" It could include credit or identity theft monitoring, fraud detection and assistance, identity theft restoration, related insurance or some other assistance. What other breach services, if any, does it also cover? If the offering is "required", what is the breadth of services required?

On September 30, 2014, California Governor Jerry Brown signed the amendments (Assembly Bill No. 1710) into law, to become effective January 1, 2015.

New Breach Notice Content Requirements

California law, as amended, will continue to require anyone conducting business in California that owns or licenses computerized data which includes personal information, to disclose a security breach to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Under the amendments, if the person or business providing notice "was the source of the breach," and if the breach exposed or may have exposed a person's Social Security number, or driver's license or other California ID, the breach notice must include "the following information," in addition to other, currently required content:

> "…an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided to the affected person at no cost for not less than 12 months…"

A plain reading of this new language, and its placement within the breach notice content requirement, would indicate that, in these cases, any offer to provide identity theft prevention and mitigation services to the affected person must be provided at no cost for at least 12 months.

A debate is brewing over whether this notification content requirement could or should be construed to require the offer of identity theft prevention and mitigation services. Such a reading, some assert, would seem to read out the words "if any." If the new content requirement is construed to mandate the offer of identity theft prevention and mitigation services in the event of certain data security breaches, California would be breaking ground as the first to require such services by legislation. The California Attorney General's office may

provide its own interpretation of the scope of this new requirement, and the Attorney General's construction may soon become clear by the time the statute becomes effective at the beginning of 2015.

The industry practice seems to have settled already on at least 12 months of free services, regardless of the type, to remediate the effects of a breach and to protect against identity theft.

In addition, for many years such services have been requested or demanded, at least in some circumstances, by state attorneys general reviewing the adequacy of breach response and the possibility of enforcement action. In some circumstances, however, breached entities do not opt to offer such services because they were not required or did not seem to be appropriate to the specific breach. Whether that will change as a result of the new California law remains to be seen. The landscape is also changing with additional breach products and services being made available – and more to come in the future – which the California law seems to have anticipated by its choice of wording.

The Expansion of Safeguard Requirements to Those who "Maintain" PI

The amendments expand the existing safeguard requirements previously applicable to "a business that owns or licenses personal information about a California resident." Similar to the HITECH amendments, the California amendment extends these requirements to include businesses that "maintain" such personal information, which would also include a number of third parties, processors and other service providers. Effective January 1, businesses that own, license *or maintain* personal information about a California resident are required by statute to implement reasonable security procedures and practices appropriate to the nature of the information, and to protect personal information from unauthorized access, destruction, use, modification, or disclosure.

Under the amended statute, entities that own, license, or maintain PI of California residents must also *contractually* require that any other third parties to whom they disclose such information (i.e., third parties that are not themselves subject to the statutory safeguard obligation) also implement and maintain the safeguards.

New Protections for Social Security Numbers

The amendment also expands the protection afforded Social Security numbers. Currently, a person or entity is prohibited (with specified exceptions), from publicly posting or displaying an individual's SSN, or doing certain other acts that might compromise the security of an SSN, unless otherwise required by federal or state law. Effective January 1, the law also prohibits selling, advertising for sale, or offering to sell an individual's SSN. Exceptions to this new prohibition include a release of an SSN incidental to a larger transaction and necessary to accomplish a legitimate business purpose, or as specifically authorized by law. Releases of SSNs for marketing purposes are not permitted.

ACTION ITEM: Review Your Response Plans, Safeguards, and Use of SSNs

Businesses that own, license or maintain personal information of California residents are affected by these amendments to the California breach notice and safeguard requirements, and restrictions on the sale of SSNs. Consider reviewing and updating accordingly your privacy, security and incident response programs and policies in order to maintain compliance. Until there is further clarification of the new breach notice content requirement, where the business is the cause of a breach involving SSNs or drivers' or other California ID numbers, it must consider the risk that certain services may be required to be offered at no cost for at least a year. Vendors should also be aware that the amendment now directly subjects them to the California requirement to safeguard personal information about a California resident.

For more information, please contact the authors of this advisory Ellen M. Giblin, Counsel, +1 617 239 0484, egiblin@edwardswildman.com, Ted Augustinos, Partner, +1 860 541 7710, taugustinos@edwardsiwildman.com, Laurie Kamaiko, Partner, +1 212 912 2768, lkamaiko@edwardswildman.com, Mark E. Schreiber, Partner, +1 617 239 0585, mschreiber@edwardswildman.com, Tom J. Smedinghoff, Partner, +1 312 201 2021, tsmedinghoff@edwardswildman.com, Karen L. Booth, Associate, +1 860 541 7714, kbooth@edwardswildman.com or one of the attorneys listed below:

Mark E. Schreiber, Partner, Chair, Steering Committee, Privacy and Data Protection Group	+1 617 239 0585	Boston	mschreiber@edwardswildman.com
Theodore P. Augustinos, Partner, Steering Committee, Privacy and Data Protection Group	+1 860 541 7710	Hartford	taugustinos@edwardswildman.com
Laurie A. Kamaiko, Partner, Steering Committee, Privacy and Data Protection Group	+1 212 912 2768	New York	lkamaiko@edwardswildman.com
Sarah Pearce, Partner, Steering Committee, Privacy and Data Protection Group	+44 (0) 20 7556 4503	London	spearce@edwardswildman.com

Barry J. Bendes, Partner	+1 212 912 2911	New York	bbendes@edwardswildman.com
Michael P. Bennett, Partner	+1 312 201 2679	Chicago	mbennett@edwardswildman.com
Nicholas Bolter, Partner	+44 (0) 20 7556 4380	London	nbolter@edwardswildman.com
Mark Deem, Partner	+44 (0) 20 7556 4425	London	mdeem@edwardswildman.com
Edward Glynn, Partner	+1 202 478 7069	Washington, DC	eglynn@edwardswildman.com
Edwin M. Larkin, Partner	+1 212 912 2762	New York	elarkin@edwardswildman.com
Stephen M. Prignano, Partner	+1 401 276 6670	Providence	sprignano@edwardswildman.com
Ronie M. Schmelz, Partner	+1 310 860 8708	Los Angeles	rschmelz@edwardswildman.com
Lisa Simmons, Partner	+1 312 201 2503	Chicago	lsimmons@edwardswildman.com
Thomas J. Smedinghoff, Partner	+1 312 201 2021	Chicago	tsmedinghoff@edwardswildman.com
David S. Szabo, Partner	+1 617 239 0414	Boston	dszabo@edwardswildman.com
David L. Anderson, Counsel	+1 310 860 8710	Los Angeles	danderson@edwardswildman.com
Patrick J. Concannon, Counsel	+1 617 239 0419	Boston	pconcannon@edwardswildman.com
Ellen M. Giblin, Counsel	+1 617 239 0484	Boston	egiblin@edwardswildman.com
Karen L. Booth, Associate	+1 860 541 7714	Hartford	kbooth@edwardswildman.com
Zachary Lerner, Associate	+1 212 912 2927	New York	zlerner@edwardswildman.com
Haley Morrison, Associate	+1 617 239 0818	Boston	hmorrison@edwardswildman.com
Ari Moskowtiz, Associate	+1 202 939 7934	Washington, DC	amoskowitz@edwardswildman.com
Matthew Murphy, Associate	+1 401 276 6497	Providence	mmurphy@edwardswildman.com
Jamie Notman, Associate	+1 617 235 5303	Boston	jnotman@edwardswildman.com
Erin Pfaff, Associate	+1 310 860 8717	Los Angeles	epfaff@edwardswildman.com
Nicholas Secara, Associate	+1 212 912 2785	New York	nsecara@edwardswildman.com
Ajita Shah, Associate	+44 (0) 20 7556 4385	London	ashah@edwardswildman.com
Kayla Tabela, Associate	+1 617 239 0734	Boston	mtabela@edwardswildman.com
Nora A. Valenza-Frost, Associate	+1 212 912 2763	New York	nvalenza-frost@edwardswildman.com

EDWARDS WILDMAN