October 9, 2014

Breaking Old Ground: California Again Amends Breach Law

By Nathan D. Taylor and Patrick Bernhardt

Not to be outdone by Florida, California has yet again amended its breach law and again in groundbreaking (yet confusing) fashion. On September 30, 2014, California Governor Brown signed into law a bill ("AB 1710") that appears to impose the country's first requirement to provide free identity theft protection services to consumers in connection with certain breaches. The law also amends the state's personal information safeguards law and Social Security number ("SSN") law. The amendments will become effective on January 1, 2015.

FREE IDENTITY THEFT PROTECTION SERVICES REQUIRED FOR CERTAIN BREACHES

Most significantly, AB 1710 appears to amend the California breach law to require that a company offer a California resident "appropriate identity theft prevention and mitigation" services, at no cost, if a breach involves that individual's name and SSN, driver's license number or California identification card number. Specifically, AB 1710 provides, in pertinent part, that if a company providing notice of such a breach was "the source of the breach":

> an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached.

The drafting of this requirement is far from clear and open to multiple readings. In particular, the use of the phrase "if any" can be read in multiple ways. For example, the phrase "if any" can be read to modify the phrase "appropriate identity theft prevention and mitigation services." Under this reading, the law would impose an obligation to provide free identity theft protection services if any such services are appropriate. The phrase "if any," however, could be read to modify the "offer" itself. Under this alternate reading, the law would provide that if a company intends to offer identity theft protection services, those services must be at no cost to the consumer. It is difficult to know how the California Attorney General ("AG") or California courts will interpret this ambiguity. One thing is clear: until the AG or courts opine, the standard will remain unclear.

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Peter Day (650) 813-4231
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
William L. Stern (415) 268-7637
Nancy R. Thomas (213) 892-5561
David M. Walsh (213) 892-5262

New York
Cindy Abramson (212) 336-4178
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Michael B. Miller (212) 468-8009
Sotirios Petrovas (212) 336-4377
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
Patrick Bernhardt (202) 887-8771
L. Richard Fischer (202) 887-1566
Adam J. Fleisher (202) 887-8781
D. Reed Freeman, Jr. (202) 887-6948
Libby J. Greismann (202) 778-1607
Julie O'Neill (202) 887-8764
Cynthia J. Rich (202) 778-1652
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

EUROPE

Berlin
Hanno Timner 49 30 72622-1346

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364
Alja Poler De Zwart 32 2 340 7360

London
Ann Bevitt 44 20 7920 4041
Amy Collins 44 20 79204180
Susan McLean 44 20 79204045

ASIA

Beijing
Gabriel Bloch 86 10 5909 3367
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Singapore
Daniel P. Levison 65 6922 2041

Tokyo
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

The drafting of the requirement also is not clear in other ways. For example, the statute does not specify what type of services would qualify as "appropriate identity theft prevention and mitigation services." For example, would a credit monitoring product alone be sufficient to meet the requirement? Or would the law require something in addition to credit monitoring, such as an identity theft insurance element?

Nonetheless, state AGs historically have encouraged companies to provide free credit monitoring to consumers following breaches. In addition, even though not legally required, free credit monitoring has become a common practice, particularly for breaches involving SSNs and also increasingly for high-profile breaches. Nonetheless, California appears to be the first state to legally require that companies offer some type of a free identity theft protection service for certain breaches.

AB 1710 is particularly notable in its approach. First, the offer of free identity theft protection services will only be required for breaches involving SSNs, driver's licenses or California identification card numbers. In this regard, an offer of free identity theft protection services will not be required for breaches involving other types of covered personal information, such as payment card information or usernames and passwords. This approach endorses a position that many companies have long held—that credit monitoring is appropriate only when the breach creates an actual risk of new account identity theft (as opposed to fraud on existing accounts). In addition, the offer of free identity theft protection services will only be required for a period of one year (as opposed to, for example, two years). The length of the offer of free credit monitoring has always been an issue of debate, and California has now endorsed a position that a one-year offer is sufficient.

SERVICE PROVIDERS DIRECTLY SUBJECT TO SAFEGUARDS REQUIREMENTS

AB 1710 also amends the California personal information safeguards law to impose the state's safeguards obligations directly on entities who "maintain" information, even if they do not own that information. The state's safeguards standard historically required companies that "own or license" covered personal information about California residents to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" in order to protect the personal information from unauthorized activity. The existing standard did not apply directly to third parties, such as service providers, that maintain information, but do not own it. Instead, the existing standard required that owners of personal information contractually require nonaffiliated third parties to whom they would disclose such information to take steps to protect the information.

AB 1710, however, specifically amends the safeguards law to impose its reasonable security procedures and practices standard directly on entities that "maintain" covered personal information, even if they do not "own or license" the data. Moreover, AB 1710 eliminates the requirement to pass-through security obligations by contract to certain third parties. Specifically, AB 1710 provides that the third-party contract requirement does not apply to a company that provides covered personal information to a third party that will now be directly subject to the safeguards standard (*i.e.*, a third party that "maintains" covered personal information). As a result, the third-party contract requirement would appear to apply only when a company discloses covered personal information to a nonaffiliated third party that will handle such data, but not "maintain" it.

NEW PROHIBITION ON SALE OF SSNS

Finally, AB 1710 amends the California SSN law to prohibit any person from selling, advertising for sale or offering to sell an individual's SSN. Moreover, AB 1710 specifically provides that the "[r]elease of an individual's

[SSN] for marketing purposes is not permitted." This new prohibition on the sale of SSNs, however, will not apply: (1) if the disclosure of the SSN is incidental to a larger transaction and is necessary to identify the individual in order to accomplish a legitimate business purpose; or (2) for a purpose specifically authorized or allowed by federal or state law. Although AB 1710's limitation on the sale of SSNs is unique among the many state SSN laws, other state SSN laws do include similar prohibitions, such as the Alaska, Minnesota, North Carolina, South Carolina and Vermont laws.

PRACTICAL IMPLICATIONS FOR BUSINESSES

The California requirement regarding free identity theft protection services for certain breaches adds yet another layer of complexity for a company that suffers a breach. Companies should be prepared to make difficult decisions regarding how to implement the new requirement. For example, companies should consider:

- Until further guidance is provided by the AG or courts, how will your company interpret the language of the requirement? For example, will your company take the position that AB 1710 does not actually impose a requirement to offer free identity theft protection services?
- What type of "appropriate identity theft prevention and mitigation" services will your company offer when it believes such an offer is required?
- In the event of a breach involving information regarding residents of multiple states, including California, will your company extend an offer of identity theft protection services to residents of states other than California?
- Will your company offer identity theft protection services in connection with breaches involving personal information other than SSN, driver's license number or California identification card number?
- When your company offers free identity theft protection services, will it provide the offer only for one year? Are there circumstances in which your company will extend an offer for a longer period?

As has been historically true, other states may follow California's lead. As a result, it will be important to monitor state legislative developments, and if a state imposes a similar requirement, determine if it follows a risk-based approach similar to AB 1710.

In addition, companies that provide services to others that involve maintaining personal information relating to California residents that is maintained but not owned should be aware that they will be directly subject to the requirements of the California safeguards law. Before AB 1710's new requirements become effective, such companies should take a fresh look at their security procedures and practices and consider whether they are appropriate and would comply with the California safeguards requirement.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and follow us on Twitter @MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.