KING & SPALDING

Client Alert

Privacy & Information Security Practice Group

November 13, 2013

California Expands Its Privacy Laws Regarding Data Breach Notice

In less than two months, when S.B. 46 becomes effective on January 1, 2014, California will extend its data breach notification requirements to a new area: individual online user accounts. Clients should take note of this significant development. It is a substantial enlargement of the notification burdens that many companies face (in particular, companies that conduct business in California and that own or license computerized data including personal information), and is indicative of, and may prefigure, other jurisdictions' efforts to update their privacy laws to ensure online privacy in emerging areas.

S.B. 46 Broadens California's Current Data Breach Notification Requirements

Under current California law, a business that owns or licenses computerized "personal information" must "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."[1] "Personal information" means "an individual's first name or first initial and last name" in combination with one or more additional data elements.[2] These data elements include a variety of individual identifiers: social security numbers; driver's license or state identification card numbers; bank-, credit-, or debit-card numbers (when combined with the account's access or security code, or password); medical information; and health insurance information.[3] "Personal information" does not include information that is publicly available through federal, state, or local government records.[4]

S.B. 46 amends and expands California's data breach notification laws to provide privacy protections for residents in a new sphere, namely, online user accounts. To achieve this, the new law broadens California's definition of "personal information." More specifically, under S.B. 46, "personal information" will include "a user name or email address, in combination with a password or security question and answer that would permit access to an online account."[5]
In addition, under S.B. 46, the kind of notification that businesses will be required to provide affected persons depends on the kind of personal information that is lost in a data breach. Where an online account is breached but none of the data elements noted above is lost (for example, there is no

For more information, contact:

J.C. Boggs
+1 202 626 2383
jboggs@kslaw.com

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

John A. Drennan
+1 202 626 9605
jdrennan@kslaw.com

King & Spalding
Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

loss of the user's first and last names in combination with, say, his or her social security number), businesses may notify the account user through the online account.[6] In such a case, the business would simply direct the user to change his or her account password and/or security questions or answers or, where applicable, to take other appropriate steps.[7]

In contrast, where there has been a breach of the "login credentials for an email account furnished by . . . the business," it is possible that an unauthorized person will have assumed control of the user account, rendering notification through the account ineffective or counterproductive. To guard against this, S.B. 46 provides that in such circumstances, businesses may not comply with their legal obligations by giving "notification to that email address," but instead must give notice in other ways (*e.g.*, though written notice, or, in certain situations, a substitute form of notice, such as a conspicuous posting on the business's Internet Web site page).[8] Businesses may also comply with their notice obligations in these circumstances by providing "clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account."[9]

Recommendations

S.B. 46 becomes effective on January 1, 2014. Companies or organizations that conduct business in California and that own or license computerized data including personal information may need to review their privacy and data security procedures to ensure that they meet the new requirements of S.B. 46.

Clients should also be aware that S.B. 46 could be seen as a model for legislation in other states (or even the federal government) to address the emerging data security issues related to online user accounts. Since 2002, forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving some form of personal information.[10] S.B. 46 will continue to fuel that trend, perhaps giving impetus to other jurisdictions to amend their data breach notification requirements. State laws in this area vary considerably, but at a minimum, S.B. 46 foreshadows further expansions of, and complications in, states' privacy laws.

If you have any questions regarding this or related issues, please contact J.C. Boggs at +1 202 626 2383, Alexander Haas at +1 202 626 5502, or John A. Drennan at +1 202 626 9605.

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Privacy & Information Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements businesses face when handling personal and other sensitive information in the U.S. and globally. This often involves assisting clients in responding to data security breaches, complying with security breach notice laws, avoiding potential litigation arising out of internal and external data security breaches, and, as necessary, defending litigation—often in the form of proposed class actions brought on behalf of those affected by a data compromise.

With more than 30 Privacy & Information Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, and public policy.

Collectively, the members of King & Spalding's Privacy & Information Security Practice have unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents, interfacing with credit card processors and card brands, engaging in complex civil litigation such as class actions, handling both state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of state and federal government.

* * *

---

[1] Cal. Civ Code §1798.82(a).
[2] *Id*. § 1798.82(h).
[3] *Id*. § 1798.82(h)(1)-(5).
[4] *Id*. § 1798.82(5)(i)(1).
[5] Cal. Civ. Code § 1798.82(h)(2) (amended 2013, effective January 1, 2014).
[6] *Id.* § 1798.82(d)(4).
[7] *See id.*
[8] *See id.* § 1798.82(j)
[9] *See id.* § 1798.82(d)(5).
[10] See National Conference of State Legislatures, State Security Breach Notification Laws, available at **http://www.ncsl.org/issues-research/telecom/security-breach-legislation-2012.aspx**. As of mid-2013, Alabama, Kentucky, New Mexico, and South Dakota did not have notification statutes for personal information breaches.