

# Morrison & Foerster Client Alert

May 18, 2015

## MoFo Privacy Minute

### Nevada Expands Definition of PI for Purposes of the State's Breach and Safeguards Laws

By Nathan Taylor

Nevada's recently amended law will, among other things, create the first state mandate to encrypt online account credentials. Specifically, on May 13, 2015, Nevada Governor Sandoval approved a bill ("AB 179") to expand the definition of "personal information" for purposes of the state's security breach notification and personal information safeguards laws. In so doing, Nevada became the fifth state this year to amend (*i.e.*, expand) the scope and obligations of its state breach law. Montana, North Dakota, Washington and Wyoming have also expanded their respective breach laws this year. Other states, such as California and Illinois, continue consideration of significant amendments to their respective breach laws.

Effective July 1, 2015, AB 179 will expand the definition of "personal information" for purposes of the Nevada breach and safeguards laws to include an individual's first name or initial and last name in combination with the following new data elements:

- (1) driver authorization card number;
- (2) medical identification number or health insurance identification number; or
- (3) user name, unique identifier or e-mail address in combination with a password, access code or security question and answer that would permit access to an online account.

#### IMPACT

The big news in this amendment is the impact this will have on the data security safeguards required for companies that handle personal information relating to Nevada residents. While several states have recently expanded their breach laws to cover online account credentials (see California, Florida and Wyoming), the same cannot be said for state safeguards laws. The Nevada amendment is significant because the state's encryption requirements will now apply to these

#### UNITED STATES

##### California

Tiffany Cheung	(415) 268-6848
Kimberly R. Gosling	(858) 314-5478
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
Stephanie Sharron	(650) 813-4018
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
Libby J. Greismann	(202) 778-1607
Julie O'Neill	(202) 887-8764
Cynthia J. Rich	(202) 778-1652
Nathan David Taylor	(202) 778-1644

#### EUROPE

##### Berlin

Hanno Timmer	49 30 72622-1346
Lokke Moerel	44 20 79204054
Alex van der Wolk	44 20 79204054

##### Brussels

Karin Retzer	32 2 340 7364
Alja Poler De Zwart	32 2 340 7360

##### London

Susan McLean	44 20 79204045
--------------	----------------

#### ASIA

##### Beijing

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

## Client Alert

---

new data elements. What that means is that companies will *not* be able to do the following with respect to online account credentials (and other “personal information” for purposes of the Nevada law, including the additional data elements added by AB 179):

- (1) transfer “personal information” through an electronic, non-voice transmission (other than a fax) to a person outside of the company’s secure system unless the transmission is encrypted in accordance with certain standards; or
- (2) move a “data storage device” containing “personal information” beyond the logical or physical controls of the company or its data storage contractor unless the information is encrypted.

### **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](http://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 our [practice page](#) 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.*