Big changes coming for post-data breach protections

James J. Giszczak, Dominic A. Paluzzi | Friday, September 21, 2018

Important consumer protection requirements designed to better safeguard consumers from identity theft in the wake of data breaches have recently been enacted, and businesses should take note.

Free credit security freezes for consumers

Effective Sept. 21, 2018, federal law now requires consumer reporting agencies such as Equifax, TransUnion, and Experian to provide free credit security freezes to consumers nationwide. Prior to this new law, costs to place and lift a freeze often ranged from $5 to $15 per credit bureau.

Previously, states such as California and New York prohibited consumer reporting agencies from charging victims of identity theft for placing freezes on their credit files. Other states like New Jersey prohibited consumer reporting agencies from charging individuals to place a security fee regardless of the circumstances, but allowed the agencies to charged consumers for permanently or temporarily lifting freezes. Still other states such as Florida and South Dakota prohibited consumer reporting agencies from charging consumers within certain age groups. Now, security freezes can be placed and lifted for free by U.S. residents, through the three credit reporting agencies.

24 months of identity monitoring services for Connecticut residents

Effective Oct. 1, 2018, Connecticut will require entities that suffer data breaches to provide Connecticut residents whose Social Security numbers were impacted by the data breach with 24 months of

complimentary identity monitoring services.

Connecticut's new requirement did not surprise many. Indeed, while Connecticut previously required businesses to provide identity monitoring services for a period of 12 months, the Connecticut Attorney General routinely asked businesses to voluntarily provide 24 months of such services.

What does this mean for businesses?

- In the immediate future, organizations should be mindful of these changes when explaining what impacted consumers can do to protect themselves in the aftermath of a breach.
- This is the time to update your incident response plan to account for these changes.
- In the more distant future, organizations should be on alert for ever expanding post-breach remediation obligations going forward. History within the privacy space has shown us that when one state comes out with sweeping regulatory changes, many states often follow.

If you have questions regarding what your organization must do to become compliant with state and federal data privacy laws, and the appropriate remedies for impacted consumers, please contact one of the attorneys below.

James J. Giszczak

Dominic A. Paluzzi