Spotlight on Data Security

Description

As seen in *Providence Business News,* June 17, 2016.

Crossing your fingers and hoping you are not hit with a cyber attack is not the best line of defense for any business. Recent government enforcement actions, particularly in the financial-services industry, make it clear that hackers are not the only eyes scanning your security protocols and safeguards.

Data breaches are ubiquitous, with claims arising from the simple negligence of lost smartphones to the more egregious intentional acts of disgruntled employees taking personally identifiable information with them on the way out the door. If your business holds any personally identifiable information, you need to take stock of your security systems, assess your risks and institute protections that are consistent and appropriate for the data you control. Failure to do so could adversely affect your business, even if no data breach has occurred.

Two recent decisions should serve as a wakeup call for all businesses regarding the need for diligence in protecting consumers' personal information.

In the Matter of Dwolla Inc., 2016-CFPB-0007 (March 2, 2016), the Consumer Financial Protection Bureau entered into a consent order with Dwolla to resolve issues related to Dwolla's data-security systems. Specifically, the CFPB charged Dwolla with deceptive acts and practices relating to representations it made regarding its data-security practices. These alleged deceptive acts and practices were enforced despite no known data breach having occurred.

The CFPB found that, in order to access its services, Dwolla required members to submit their name, address, date of birth, telephone number and Social Security number, as well as bank account and routing numbers, pin numbers, passwords and usernames. This consumer information was collected and stored by Dwolla. The CFPB did not find Dwolla's collection of information troublesome in and of itself. Instead, the CFPB scrutinized the data-security Dwolla was representing it had created versus the systems it actually had established and found Dwolla liable for not meeting the standard of care it had represented to its customers as being in place.

The CFPB examined Dwolla's data-security systems and found them deficient. According to the CFPB, Dwolla's systems did not provide the security it advertised. CFPB concluded that Dwolla's members were materially misled, even though no data breach had occurred. As a result, Dwolla and the CFPB entered into a consent order which, in addition to a penalty of $100,000, required Dwolla to take several affirmative actions to implement appropriate data-security measures to protect consumers' personal information.

In another case, the New York Department of Financial Services, Financial Frauds & Consumer Protection Division, entered into a consent order with Blue Global. Similar to the Dwolla matter, NYDFS alleged that Blue Global made misrepresentations in its marketing materials, including statements that it had authority to conduct business in New York (which it did not) and that it was adequately equipped to protect its New York consumers' personal information. The consent order imposed a penalty of $1,000,000 against Blue Global and granted the NYDFS injunctive relief to restrict Blue Global's activities in other ways.

Making sure you have proper insurance, procedures, policies, training, contractual terms with third parties and other systems in place is now more critical than ever to reduce the risk of enforcement actions that can be time-consuming and expensive.

Date Created
June 17, 2016