NEWSSTAND

Data Security Developments for the Insurance Industry

March 2010
Theodore P. Augustinos, Karen L. Booth

In this article, we briefly review several recent developments in the data security requirements that affect insurance companies and producers with operations in the United States and Europe. The issue of data security is increasingly important to insurers and producers, as data breaches, and related fines and litigation, are revealed on a regular, almost daily basis. Insurance companies and producers have their own burdens and exposures relative to the personal information[1] of their insureds, employees and agents. They also have opportunities to offer coverage to other companies that have exposure to data security risks.

January 1, 2010
State requirements in the US continue to evolve. On January 1, 2010, a new amendment to the Nevada privacy law became effective. This amendment requires any company doing business in Nevada that accepts payment cards to comply with the Payment Card Industry Data Security Standards (PCI DSS). Prior to this amendment, the obligations of PCI DSS to secure certain personal information of payment card users were imposed contractually by the payment card industry to require encryption and other onerous safeguards. Violations of the these standards were subject to fines and other contractual sanctions. With the Nevada amendment, however, these standards are now also imposed by law. In addition, the amendment requires companies doing business in Nevada that may not accept payment cards, but otherwise collect data, to adopt encryption technologies to protect certain stored and transmitted data.

February 17, 2010
Effective February 17, 2010, the reach of the HITECH Act will be expanded to impose substantial parts of the HIPAA privacy and security requirements related to the protection of health information directly on "business associates," which are defined to include any person providing services to a healthcare provider involving the use or disclosure of individually identifiable health information. The newly effective provisions of the HITECH Act also restrict the use and disclosure of protected health information for marketing purposes and contain other amendments. By the effective date for these provisions, covered entities should consider putting new business associate agreements in place to reflect these new privacy and security requirements, as well as data breach notification obligations.

February 22, 2010
HIPAA imposes a breach notification requirement for covered entities and business associates, and for personal health record vendors and their contractors, which will be fully enforced beginning February 22, 2010.

March 1, 2010
On March 1, 2010, the Massachusetts Security Regulation is scheduled to take effect, after several postponements and amendments. While requirements for encryption and certain other technical requirements have been relaxed since this Regulation was first proposed, the basic requirements for any company or person that owns or licenses certain personal information of any Massachusetts resident remain specific and relatively burdensome. These requirements apply regardless of whether the company is doing business in Massachusetts. Central to the Massachusetts Security Regulation is the requirement that each such company adopt a Written Information Security Program (WISP) containing specific elements to ensure the security of personal information.

Due to the nature of these requirements, most companies and persons owning or licensing personal information of any Massachusetts resident, whether because they have one or more Massachusetts employees, agents or insureds, or otherwise, are making a corporate-level decision to comply with these requirements nationally, and in some cases globally, because the cost and risk related to culling out personal information of Massachusetts residents and treating it differently from other information owned or licensed by the company is too high.

It should also be noted that under the Massachusetts Security Regulation, companies and persons must amend their vendor contracts pursuant to which certain personal information of Massachusetts residents is transmitted to and stored or processed by vendors. Contractual provisions requiring compliance with the Massachusetts Security Regulation must be included in contracts entered into on or after March 1, 2010. Contracts entered into before that date must be amended to comply by March 1, 2012.

June 1, 2010
The Red Flags Rule promulgated by the Federal Trade Commission requires that financial institutions (essentially banking institutions) and "creditors" that maintain "covered accounts" develop and implement written Identity Theft Prevention Programs to detect, prevent and mitigate identity theft. For this purpose, "creditors" and "covered accounts" are very broadly defined, and would include insurance companies and producers that provide insurance coverage and bill premiums afterward, whether or not interest is charged. While financial institutions have had to comply with the Red Flags Rule since November 28, 2008, creditors that maintain covered accounts must comply by June 1, 2010.

Unlike the specific requirements of the Massachusetts Security Regulation, the approach of the Red Flags Rule is much more flexible, but very comprehensive. There are no specific technologies, techniques or contractual requirements, for example, but creditors must implement a comprehensive program that would detect, prevent and mitigate identity theft.

European Developments
In addition to complying with US data protection, most US insurance companies and producers with subsidiaries in the European Union need to be aware of the data protection laws in the EU, enforcement, and the penalties for non-compliance. There are new penalties for data protection violations and breaches in Germany, and a recent increase in penalties in the UK, as noted below. Further, those publicly traded firms implementing whistleblowing programs for

subsidiaries in the EU in order to comply with two important US laws, the Sarbanes-Oxley Act of 2002 and the Foreign Corrupt Practices Act, should also take note of recent important whistleblower decisions, guidelines or directions in France, Denmark, Sweden, Portugal, Austria, and Hungary.

The Information Commissioner's Office (ICO) in the UK has recently been granted increased statutory powers to impose fines up to £500,000. The new powers, which are expected to come into force on April 6, 2010, apply when the ICO is satisfied that: (i) there has been a serious breach of one or more of the data protection principles of the organizations; and (ii) the breach was likely to cause substantial damage/distress, i.e., if the breach was deliberate or the organization knew or should have known there was a risk, such as by the reckless handling of personal data. As some data breaches may include individual names in other countries, the fine levels of those authorities becomes increasingly important.

The German Federal Parliament passed comprehensive amendments to the Federal Data Protection Act, effective September 1, 2009, that cover a broad variety of data protection issues and give fine authority of € 50,000 for simple violations and € 300,000 for serious violations. The data protection authorities have been given these new powers to enable them to impose higher fines for failure to comply with data protection requirements, especially on the security side.

---

[1] For purposes of this article, we use the term personal information to include the financial, health and other nonpublic personal information generally covered by these federal and state requirements.