

## **Commission Statement Marking the FTC's 50th Data Security Settlement January 31, 2014**

Today marks a milestone for the Federal Trade Commission – the announcement of the Commission's 50<sup>th</sup> data security settlement. What started in 2002 with a single case applying established FTC Act precedent to the area of data security has grown into a vital enforcement program that has helped to increase protections for consumers and has encouraged companies to make safeguarding consumer data a priority.

Congress charged the FTC with responsibility for protecting consumers from deceptive and unfair commercial practices across many sectors of the economy, which it does principally through enforcement of Section 5 of the FTC Act. Since 2002, under the leadership of Chairman Timothy Muris, and during the subsequent tenures of Chairmen Deborah Platt Majoras, William Kovacic, and Jon Leibowitz, and continuing today, the Commission has used this authority to protect millions of consumers from unfair or deceptive practices that put their personal information at risk. The Commission's fifty data security settlements have halted harmful data security practices; required companies to accord stronger protections for consumer data; and raised awareness about the risks to data, the need for reasonable and appropriate security, and the types of security failures that raise concerns. And they have addressed the risks to a wide variety of consumer data, such as Social Security numbers, health data, data about children, credit card information, bank account information, usernames, and passwords, in a broad range of sectors and platforms, including retail, financial, mobile, and social media.

The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

The Commission has also provided educational materials to industry and the public about reasonable data security practices. These materials explain that, while there is no single solution, such a program follows certain basic principles. First, companies should know what consumer information they have and what employees or third parties have access to it. Understanding how information moves into, through, and out of a business is essential to assessing its security vulnerabilities. Second, companies should limit the information they collect and retain based on their legitimate business needs so that needless storage of data does not create unnecessary risks of unauthorized access to the data. Third, businesses should protect the information they maintain by assessing risks and implementing protections in certain key areas – physical security, electronic security, employee training, and oversight of service providers. Fourth, companies should properly dispose of information that they no longer need. Finally, companies should have a plan in place to respond to security incidents, should they occur.

We live in an increasingly connected world, and data security is of critical and growing importance to consumers. The Commission will continue its efforts to educate businesses on reasonable data security practices to help them prevent future breaches from occurring. The Commission's body of fifty data security settlements reflects its commitment to ensure that companies employ reasonable measures to safeguard consumer data. As the Commission moves forward, it will continue to hold companies accountable for practices that violate the law by falling short of this standard.