

## FTC and Department of Health and Human Services Settle with CVS over Allegations that the Company Failed to Protect the Privacy of Customer and Employee Personal Information

*On February 18, 2009, the FTC announced that it settled with CVS Caremark Corporation (“CVS Caremark”), the parent company of CVS Pharmacy, over allegations that the company failed reasonably to protect the sensitive financial and medical information of its customers and employees. The FTC brought the action together with the Office of Civil Rights (“OCR”) of the Department of Health and Human Services (“HHS”).*

Under the settlement, CVS Pharmacy will pay \$2.25 million to HHS to settle allegations that it violated the Health Insurance Portability and Accountability Act (“HIPAA”), and both CVS Caremark and CVS Pharmacy will implement various information security procedures required under the HHS resolution agreement and the FTC consent order. This is the FTC’s twenty fourth case challenging the alleged failure by a company to implement reasonable information security practices.

This is the first FTC data security case: (1) involving a health provider, (2) proceeding jointly with HHS, and (3) challenging the security of employee data. It makes good on the FTC’s promise to bring enforcement actions involving employee data, and it shows that the FTC can and will work with other agencies to resolve security concerns. It is not unreasonable to expect that, after working with the FTC on this enforcement action, HHS will become more active in bringing enforcement actions.

### RELEVANT FACTS

CVS Caremark operates the largest pharmacy chain in the United States, with over 6,300 retail pharmacies nationwide, in addition to an online and a mail-order pharmacy business. The FTC and HHS launched simultaneous investigations after nationwide media released reports alleging that CVS Pharmacy was disposing sensitive customer and employee personal information in public dumpsters outside of its retail outlets. Specifically, the reports alleged that the company was disposing trash that contained:

- Pill bottles with patient names, addresses, prescribing physicians’ names, medication and dosages;
- Medication instruction sheets with personal information;
- Computer order information from the pharmacies, including consumers’ personal information;
- Employment applications, including Social Security numbers;
- Payroll information; and
- Credit card and insurance card data, including, in some cases, account numbers and driver’s license numbers.

This sensitive personal information included that of both customers *and* employees, and included patient health care and health insurance information.

### ALLEGATIONS

In its complaint, the FTC alleges that CVS failed to:

- Implement reasonable and appropriate procedures for handling personal information about customers and employees;

- Implement reasonable policies and procedures to securely dispose of personal information;
- Adequately train employees;
- Use reasonable measures to assess compliance with its policies and procedures for disposing of personal information; or
- Employ a reasonable process for discovering and remedying risks to personal information.

In addition, the FTC alleges that CVS Caremark's claim that "CVS/pharmacy wants you to know that nothing is more central to our operations than maintaining the privacy of your health information" is deceptive. As a result of these acts and omissions, the FTC charged that CVS Caremark violated Section 5 of the FTC Act for the misrepresentation of its pharmacy's privacy practices and for maintaining unfair security practices.

The HHS OCR alleged that CVS Pharmacy violated the HIPAA Privacy Rule, which requires health plans, health care clearinghouses, and most health care providers (covered entities), including most pharmacies, to safeguard the privacy of patient health information, including during disposal.

### SETTLEMENT REQUIREMENTS

Consistent with standard FTC data breach settlements, the FTC consent order requires CVS Caremark to establish, implement, and maintain a comprehensive information security program designed to protect the security, confidentiality, and integrity of the personal information it collects from consumers and employees. CVS must also pay a qualified data security auditor to audit the company's security program every other year for twenty (20) years and submit such reports to the FTC for review. In addition, the settlement bars CVS from misrepresenting the company's security practices.

Under the terms of the HHS resolution agreement, CVS Pharmacy is required to implement a Corrective

Action Plan, which specifically requires that the company establish and implement policies and procedures for disposing of protected health information, implement a training program for handling and disposing of such information, conduct internal monitoring, and engage a qualified independent assessor to evaluate compliance with the settlement for three years. CVS will also pay HHS a \$2.25 million resolution amount.

### KELLEY DRYE & WARREN LLP

Kelley Drye & Warren's Privacy and Information Security Practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

**For more information about this Client Advisory, please contact:**

**D. REED FREEMAN**

(202) 342-8880

[rfreeman@kelleydrye.com](mailto:rfreeman@kelleydrye.com)

**ALYSA Z. HUTNIK**

(202) 342-8603

[ahutnik@kelleydrye.com](mailto:ahutnik@kelleydrye.com)