

Failure to comply with the payment card industry's data security standards (the PCI standards) when accepting and processing credit/payment card transactions**Factual background**

A large multi-national brick and mortar retailer suffered a breach of its in-store payment card system when organized thieves hacked into the retailer's wireless network. As a result, between 46 million and 94 million customers' payment card information was stolen over the course of several years.

Incident response

The retailer first went public with the breach in the media, and also notified applicable regulators of the incident. It also notified by mail those customers whose personally identifiable information (in addition to their payment card information) was stolen (about 454,000 customers).

Litigation / enforcement proceedings

Following this incident, over 20 class action law suits were brought against the retailer on behalf of consumers, payment card issuing banks and shareholders. In addition, the Federal Trade Commission and at least 37 state attorneys general launched an investigation, as well as Canada's federal Privacy Commissioner, Alberta's Information and Privacy Commissioner, and the United Kingdom's Information Commissioner.

Outcome

The retailer settled the consolidated consumer class action claims, providing three years worth of credit monitoring services and identity theft insurance to customers whose personally identifying information may have been compromised, reimbursing customers for documented costs of replacing drivers licenses and addressing identity theft, issuing store vouchers or checks to some class members to reimburse expenses (up to \$7M), holding a 15% customer appreciation sale, and paying attorneys fees (up to \$6.5M) and costs and expenses (up to \$150,000). The settlement also requires the retailer to undertake an independent evaluation of its data security measures and implement data security enhancements.

The retailer settled with most of the card issuing banks who suffered the costs of unauthorized charges and reissuing new cards. The settlement amount was \$40.9 million.

The joint investigation by Canada's federal Privacy Commissioner and Alberta's Information and Privacy Commissioner resulted in a finding that the retailer had failed to comply with the PCI standards, and had violated Canada's federal Personal Information Protection and Electronic Documents Act and Alberta's Personal Information Protection Act. As a result of this investigation, the retailer implemented a new system for processing merchandise returns without a receipt, which better protects consumers' personal information.

Other suits and regulatory investigations are pending.

The retailer's SEC filings estimate the total cost of the incident to be \$156MM.

Data aggregator fell for con artists' scheme to steal consumers' sensitive personal information**Factual background**

A large data aggregator, in the business of selling credit report information about consumers to its customers, was conned into selling over 160,000 consumer records to con artists posing as legitimate business enterprises with a legitimate need and purpose for such information. The stolen consumer records contained social security numbers, financial data and other personal information. About 800 cases of identity theft were ultimately linked to the incident.

Incident response

The company notified by mail the individuals whose sensitive personal information was compromised.

Litigation / enforcement proceedings

Putative class action law suits were filed against the company on behalf of consumers whose sensitive personal information was compromised by the incident. The Federal Trade Commission and 43 state attorneys general and the District of Columbia launched investigations into the incident. A class action law suit was brought against the company on behalf of shareholders alleging that stock prices were negatively affected by the company's failure to adequately protect sensitive consumer information. The SEC launched an investigation to determine whether top company executives sold stock in advance of making the data breach incident public.



Information security breach loss scenarios

Outcome

Consumer class action law suits were dismissed.

The company settled the FTC's action for \$10M in fines and up to \$5M for consumer redress. The company also agreed to establish and maintain an information security program, which will be audited by a third party security professional every two years until 2026. The company's SEC filings estimate the cost of the information security program to be \$4M.

The company entered into an agreement with 43 state attorneys general and the District of Columbia, agreeing to strengthen safeguards for consumers' personally identifiable information and to pay \$500,000 to the various states to cover the costs of their investigation.

Three years after the breach, the company settled the shareholder class action law suit for \$10M, and the SEC closed its investigation into the incident without filing charges.

The company's SEC filings estimate the total cost of the incident to be \$33.8MM over the course of three years.

A large retailer's payment card processing system was hacked into by criminals

Factual background

Payment card issuing banks began to notice a correlation between payment cards that were used to make authorized purchases at this retailer's store and cards that were subsequently used to make unauthorized purchases at other stores. It was then discovered that the retailer's payment card processing system suffered from vulnerabilities that allowed culprits to hack in and steal payment card information. They used the stolen information to manufacture counterfeit cards that were used to make several millions of dollars worth of fraudulent purchases.

Incident response

After finding out about the incident, the retailer retained a computer security firm to conduct a forensic analysis of its information technology systems to determine whether a breach had in fact occurred. Although the forensic report was inconclusive, the retailer issued a public statement alerting consumers to the potential security breach.

Litigation / enforcement proceedings

The Federal Trade Commission launched an investigation into the incident. Also, banks and credit unions initiated law suits against the retailer.

Outcome

The retailer settled the FTC's claims, agreeing to fortify its information security policies and be subject to 20 years of oversight by the FTC. The claims by banks and credit unions against the retailer are pending, including a \$13MM damages claim.

The retailer's SEC filings estimate the total cost of the incident to be \$13MM.

Mass email sent inadvertently exposed personal medical information about individuals

Factual background

An employee of a pharmaceutical company accidentally transmitted a mass email containing personal medical information of hundreds of individuals.

Litigation / enforcement proceedings

The Federal Trade Commission launched an investigation, as well as eight state attorneys general.

Outcome

The pharmaceutical company settled the FTC's action, agreeing to establish and maintain a four-stage information security program designed to protect sensitive personal information. The company also settled claims brought by eight state attorneys general, promising to strengthen its internal standards relating to privacy protection, training and monitoring, to undergo annual independent compliance reviews for the following five years, and pay \$160,000 to the various states to settle the case.

Insecure disposal of sensitive personal information**Factual background**

A local small business routinely disposed of customer records in easily-accessible trash cans behind its stores. The records contained promissory notes and bank statements containing social security numbers, addresses, driver's license numbers and checking account information.

Litigation / enforcement proceedings

The state attorney general sued the local business for violation of state consumer protection laws. Under one cause of action, violators can be fined \$50,000 per violation. Under another, penalties can be up to \$500 per abandoned record. Under a third, fines can be up to \$25,000 per violation.

Outcome

A temporary injunction has been agreed to. Substantive claims for damages and penalties are pending.

Company failed to timely notify its client of its loss of a laptop containing consumer information**Factual background**

A services provider who, in the course of its business, processes sensitive personal information about individuals on behalf of its clients, failed to timely notify its client when it lost a laptop containing consumer information relating to 540,000 individuals. The types of personal information lost included names, addresses, and social security numbers.

Incident response

Seven weeks after finding out about the missing laptop, the company notified its client and requested assistance from the FBI. It also notified various state agencies. Weeks later, the company notified the 540,000 individuals whose sensitive personal information was contained on the laptops.

Litigation / enforcement proceedings

The state attorney general took action against the company.

Outcome

In a settlement with the state attorney general, the company agreed to comply with breach notification laws in the future, to pay \$60,000 as reimbursement of state costs, and to implement practices to protect the security of private information.