In March 2010, 28 year-old Albert Gonzalez was sentenced to 20 years in federal prison for breaching security measures at several well-known retailers and stealing millions of credit card numbers, which he then resold across a variety of shadow “carding” Web sites. Using a fairly simple packet sniffer, Gonzalez was able to steal payment card transaction data in real time, which he then parked on blind servers in places such as Latvia and Ukraine—countries formerly part of the Soviet Union. Gonzalez named his activities “Operation Get Rich or Die Tryin'” and lived a lavish lifestyle by selling stolen credit card information. He was eventually tracked down by the U.S. Secret Service, which was investigating the stolen card ring. Operation Get Rich or Die Tryin' took place for more than two years and cost major retailers, such as TJX, OfficeMax, Barnes & Noble, Heartland, and Hannaford, more than $200 million in losses and recovery costs. It is the largest computer crime case ever prosecuted.

At first glance, Operation Get Rich or Die Tryin' seems to be an open-and-shut case. A hacker commits a series of cybercrimes, is caught, and is successfully prosecuted. Fault and blame are assigned to the cybercriminal, and justice is served for the corporations and the millions of people whose credit card information was compromised.

Unless you ask the shareholders, banking partners, and some customers of TJX, who filed a series of class-action lawsuits against the company claiming that the “high-level deficiencies” in its security practices make it at least partially responsible for the damages caused by Albert Gonzalez and his accomplices. The lawsuits point out, for example, that the packet sniffer Gonzalez attached to the TJX network went unnoticed for more than seven months. Court documents also indicate that TJX failed to notice more than 80 GB of stored data being transferred from its servers using TJX’s own high-speed network. Finally, an audit performed by TJX’s payment-card processing partners found that it was noncompliant with 9 of the 12 requirements for secure payment card transactions. TJX’s core information security policies were found to be so ineffective that the judge presiding over sentencing hearing of Gonzalez reviewed them to determine whether TJX’s damages claim against him of $171 million is valid.

Apart from lawsuits, TJX faced a serious backlash from customers and the media when the details of the scope of the breaches trickled out. Customers reacted angrily when they learned that nearly six weeks had passed between the discovery of the breach and its notification to the public. News organizations ran headline stories that painted a picture of TJX as a clueless and uncaring company. Consumer organizations openly warned people not to shop at TJX stores. TJX’s reputation and brand image was shattered in the wake of Operation Get Rich or Die Tryin', and only a small portion of the damage was actually Albert Gonzalez’s fault.

The real lesson of Operation Get Rich or Die Tryin' may not be the crime itself, but how a lackluster security policy was chiefly responsible for it happening in the first place.