Why the FTC has hackers' victims in its crosshairs
Verne Kopytoff

Hackers routinely infiltrate corporate computer systems to steal customer credit card numbers and other personal data. The government punishes their victims.

Hackers infiltrate Company X's computers and make off with thousands of customer credit card numbers. After learning of the theft, Company X apologizes and promises to beef up its security. A storm of public indignation builds and then passes until, soon after, the cycle repeats itself when hackers attack another Company Y. And so on.

Only rarely does the script deviate like it did this week when the Federal Trade Commission sued Wyndham Worldwide (WYN) for failing to do enough to protect its customer information. The complaint, filed in federal court in Arizona, alleged that Wyndham did little to upgrade security after hackers breached its computer system three times in two years.

Wyndham responded that the case was without merit.

Unlike Wyndham, most companies that fall victim to hackers never enter the F.T.C.'s crosshairs. As long as businesses have reasonable security measures, they can avoid punishment after even serious breaches.

What draws the F.T.C.'s attention is when it believes a company left the door wide open to its customer information. Such inattention violates privacy policies in which companies invariably promise that they safeguard the consumer data they collect, using standard industry practices. "We have always said that it is not a violation to be hacked," said Kristin Cohen, an attorney in the F.T.C.'s division of privacy and identity protection. "We can only go after companies that have misleading privacy policies -- either they did something that was deceptive or unfair."

Over the past decade, the F.T.C. has reached settlements or sued around 35 companies for misrepresenting their data security. For example, RockYou, a social game site, settled with the agency earlier this year while Twitter did so in 2010.

The number of cases pales next to the proliferation of successful hacker attacks in the United States. Last year alone, there were 419 breaches reported affecting 22.9 million people, according to the Identity Theft Resource Center, a group that tracks the problem. The number of successful attacks is almost certainly higher, however, because many companies fail to disclose when their defenses are defeated, said Rex Davis, director of operations for the center.

In its complaint Tuesday, the F.T.C. said that Wyndham, which operates and franchises Days Inn, Super 8 and Ramada hotels, failed to implement basic security measures. Credit card numbers were stored in text files that hackers could easily read, for example.

The first hacker attack against Wyndham in 2008 compromised 500,000 credit card accounts, and led to hundreds of thousands of account numbers being sent to a domain registered in Russia. Two more attacks over the next two years accessed another 50,000 credit and debit card numbers.

The F.T.C. said that the hackers were able to use the information they obtained to make $10.6 million in fraudulent charges. Wyndham countered that it knows of no customers who suffered a financial loss.

The F.T.C.'s authority for most consumer data protection cases comes from the F.T.C. Act, and does not include the ability to levy financial penalties. Rather, the agency usually requires companies to upgrade their security, undergo regular security audits from a third-party and promise to make no more misrepresentations for 20 years.

To give it greater teeth, the F.T.C. recently asked Congress for legislation that would allow it to impose financial penalties in data security cases - much like the agency already does for other types of corporate misbehavior. A Senate bill was recently introduced with such a provision. In addition to the F.T.C., the various state attorneys general sometimes punish companies for insufficient security.

The F.T.C.'s oversight of data security does not include banks, which are instead regulated by the Federal Deposit Insurance Corporation, among others. Hackers frequently target banks, and last year, for instance, gained access to the computer system of Citigroup and stole information from more than 200,000 credit card holders.

Fonte: Fortune, 28 June 2012. Disponível em: <http://tech.fortune.cnn.com/2012/06/28/ftc-hackers/?iid=SF_F_River>. Acesso em: 28 June 2012.

A utilização deste artigo é exclusiva para fins educacionais.