Hacked Casino Sues Cybersecurity Firm

JONATHAN E. MISSNER AND ROBERT B. GILMORE REPRESENT AFFINITY GAMING IN A LAWSUIT AGAINST TRUSTWAVE.
Originally Published in The Hill

By Katie Bo Williams

January 18, 2016

A U.S. casino is suing the cybersecurity firm it hired to help handle a data breach in a case that experts say is likely the first of many.

"The cost of a data breach incident is staggering, and I think you're going to see a lot of lawsuits trying to determine who should pay the cost of an incident and trying to allocate blame for that," said Sara Romine, an attorney with Carrington, Coleman, Sloman & Blumenthal who regularly handles data security cases.

The lawsuit, filed in late December, appears to be one of the first of its kind, in which a company challenges a cybersecurity contractor on how it manages the fallout from a hack.

Affinity Gaming hired Trustwave, a Chicago-based cybersecurity firm, to investigate and remedy a 2014 breach that compromised credit card information for around 300,000 customers.

Affinity now alleges that it discovered a second hack that occurred during the investigation process — after Trustwave assured it that its systems were secure. It's suing Trustwave for misrepresenting its ability to protect Affinity's data.

"In reality, Trustwave lied when it claimed that its so-called investigation would diagnose and help remedy the data breach, when it represented that the data breach was 'contained,' and when it claimed that the recommendations it was offering would address the data breach," Affinity's complaint reads.

Trustwave has denied any wrongdoing and will defend itself in court, according to the Financial Times. The company did not respond to a request for comment by The Hill.

Until now, most high-profile cybersecurity lawsuits have been brought by victims of data theft against breached companies. The cost of such cases can be exorbitant, pushing companies to look for ways to share their responsibility.

Hacked Casino Sues Cybersecurity Firm

The massive 2013 hack of retailer Target highlights the high costs for breaches.

Target last year agreed to a $10 million settlement in a class-action suit brought by customers exposed in hack.

In addition, the company agreed in late December to a $39 million settlement to resolve claims by banks that sought to recoup money for reimbursing fraudulent charges. In August, Target agreed to pay Visa card issuers up to $67 million to resolve claims related to the hack.

Although the exact extent of fraud committed as a result of the breach isn't known, the attack had cost Target $162 million in net expenses as of Jan. 31, 2015.

The Federal Trade Commission (FTC) has also begun to take enforcement action against firms that do not adequately safeguard consumer information. The agency has brought more than 50 suits against companies over lax cybersecurity, most of which have resulted in settlements.

Such cases have created a frustrating — and expensive — complication for businesses that are themselves the direct victims of hackers, experts say.

As a result, firms facing the high costs of a data breach are beginning to look for ways to defray those costs.

"Whose responsibility was it to either detect, prevent or remediate the breach?" Romine said. "Given the cost of a data breach, there's a lot of finger-pointing over who should bear that cost."

Affinity claims that it was a "victim of Trustwave's deceptive trade practices" — it "relied on [Trustwave's] assurances" that it could remediate the breach and was "consequently and proximately harmed by Trustwave's misrepresentations and omissions."

According to Affinity, "Trustwave knew (or recklessly disregarded) that it was going to, and did, examine only a small subset of Affinity Gaming's data systems," causing it to miss the second breach entirely, despite its promises that it had shored up Affinity's networks.

Such cases will hinge on the contractual expectations of both parties, Romine says.

She notes that the allegations made by Affinity mirror the allegations brought by the FTC against businesses. Both rely on the assumption that poor cybersecurity can be considered an unfair or deceptive trade practice if the defendant has misrepresented its ability to safeguard data.

As breaches proliferate and more companies enter the lucrative cybersecurity market, Romine says, judges in these cases will look to the conversations between company and vendor to determine responsibility.

Hacked Casino Sues Cybersecurity Firm

"As you have more and more businesses that enter this space, it's going to important for all the parties to be clear on the expectations of, what it is that you're doing to ensure cybersecurity," Romine said.

But with the threat landscape shifting daily, such expectations can be difficult to nail down in court, experts say.

Critics of the FTC's claim to cybersecurity authority say that the agency has failed to lay out clear regulations for companies to follow. They say it relies instead on a vague requirement that companies provide "reasonable" protection to their customers.

Similar challenges will likely plague any case against a cybersecurity firm.

Link to Original Article: Hacked Casino Sues Cybersecurity Firm