

Can Cybersecurity Whistleblowers Receive Monetary Awards from the SEC?

By [Alexis Ronickher](#)
November 29, 2016

The viability of a cybersecurity whistleblowing tip under the [SEC Whistleblower Reward Program](#) is no longer a question. In June 2016, the SEC announced a \$1 million penalty levied against Morgan Stanley Smith Barney LLC for cybersecurity violations that, when coupled with a related criminal action, totaled \$1.6 million. We may never know whether a whistleblower provided information in this enforcement action since the SEC's policy is to strictly protect the identities of whistleblowers. What we do know is that if there were a whistleblower involved, this is the first SEC action involving cybersecurity to meet the \$1 million threshold for an award.

Legitimizing Cybersecurity Whistleblowers

Prior to June 2016, the SEC was very vocal about cybersecurity issues being a serious enforcement priority but had not pursued an enforcement action against a firm for inadequate cybersecurity. This changed on Sept. 22, 2015, when the SEC announced that R.T. Jones Capital Equities Management agreed to pay a penalty of \$75,000 for failing to maintain adequate cybersecurity. This action confirmed that the SEC would pursue enforcement actions against firms violating cybersecurity requirements. On the other hand, the small penalty amount left in doubt whether such enforcement actions could result in monetary sanctions significant enough for a whistleblower to receive an award since the SEC Whistleblower Reward Program requires monetary sanctions in an action to exceed \$1 million for a whistleblower to be eligible for an award.

Awards for Cybersecurity Whistleblowers

June 8, 2016 brought the answer as to whether [cybersecurity violations](#) could result in monetary sanctions large enough to produce an award. That's when the SEC announced that Morgan Stanley agreed to pay a \$1 million penalty for violating Rule 30(a) of Regulation S-P, known as the "Safeguard Rule," by failing to adopt written policies and procedures reasonably designed to protect customer data. Specifically, for more than 10 years, Morgan Stanley failed to have effective authorization modules that restricted employees' access to confidential customer data for two internal web applications. This failure was compounded by the firm's failure to audit or test the ineffective authorization modules, or to monitor or analyze employees' access to and use of the applications.

These cybersecurity failures had real consequences. A then-employee was able to download and transfer confidential data to his personal server between 2011 and 2014. Later, portions of that confidential data were posted online as a teaser for the sale of larger quantities of confidential data, apparently by a third party who hacked the employee's server.

A whistleblower is not eligible for an award under the SEC Whistleblower Reward Program unless the monetary sanctions collected exceeds \$1 million, a threshold that the Morgan Stanley penalty was just shy of. The SEC Whistleblower Reward Program rules, however, allow in certain circumstances for a whistleblower to aggregate the monetary sanctions collected in cases arising out of a common nucleus of operative facts. In the Morgan Stanley case, there is just such a related case. On Dec. 22,

2015, a court ordered the former Morgan Stanley employee who illegally downloaded the confidential information to pay \$600,000 in restitution, along with other penalties. Provided that the employee pays any portion of this fine, the monetary sanctions in the Morgan Stanley matter would exceed the \$1 million threshold and create a viable whistleblower award.

The Future of Cybersecurity Whistleblowers

Again, we may never know whether the SEC issued a whistleblower award related to the Morgan Stanley action. What is critical, however, is that we now know that information related to inadequate cybersecurity can result in monetary sanctions high enough to allow for such an award. Individuals who are aware of violations of the Safeguard Rules should seriously consider filing a tip with the SEC.

That being said, in both the R.T. Jones and the Morgan Stanley cases, the respective firm's failure to maintain adequate cybersecurity protections resulted in actual compromising of confidential customer information for hundreds of thousands of individuals. It is likely that for the SEC to take an enforcement action related to cybersecurity that would result in an eligible monetary sanction, a firm's cybersecurity failures would need to result in demonstrable harm to a significant number of individuals, even if that harm is limited to the compromising of their personal information.