

Ex-Morgan Stanley Adviser Pleads Guilty in Connection with Data Breach

Patrick Atchison, J.D. Candidate 2018

A former financial advisor for Morgan Stanley, Galen Marsh, pleaded guilty last week to one count of unauthorized computer access in connection with one of the largest data breaches of a private wealth management company.

Between 2011 and 2014, Marsh uploaded sensitive financial information—including names, addresses, bank account numbers, and investment information—of over 350,000 Morgan Stanley clients to his private computer.

In late 2014, data from 900 Morgan Stanley clients appeared online at Pastebin.com, an open file sharing website known for leaking confidential information, including the hacking of Sony Pictures. The breached data did not include “critical” information such as social security numbers or account passwords, but cyber security expert Darren Hayes of Pace University told the Wall Street Journal that it could provide an “important first step” for identity thieves to create duplicate identities. According to Morgan Stanley, there have been no reports of financial loss from the breach.

In January, the FBI and Financial Industry Regulatory Authority (FINRA) launched criminal investigations into Marsh’s activity, while the Federal Trade Commission (FTC) opened an investigation into Morgan Stanley’s data security procedures.

It was initially suspected Marsh posted the information online in exchange for online currency. At the time of the internet disclosures, Marsh had ongoing employment discussions with two of Morgan Stanley’s competitors. Yet, Mr. Marsh’s attorney, Robert C. Gottlieb of Gottlieb & Cordon LLP, said Marsh never posted Morgan Stanley client information online and federal regulators were looking into the possibility his personal computer was targeted by hackers after downloading the data.

The FTC determined the data breach was made possible by a glitch in Morgan Stanley’s data security controls, but did not find the company criminally liable for the breach. Maneesha Mithal, associate director of the Division of Privacy and Identity Protection at the FTC, stated that Morgan Stanley had “reasonable comprehensive (security) policies in place,” and “promptly fixed the problem when it came to the company’s attention.”

According to Bob Olson, Vice President and head of global financial services at Unisys, the Morgan Stanley data breach has “similar characteristics” to previous data breaches like those at JPMorgan Chase, Target, Home Depot, and Sony Pictures. Olson advocates that companies storing large quantities of sensitive data narrowly tailor their security policies to allow employees access only to data necessary to complete their job functions. According to the Wall Street Journal, Marsh was able to gain access to almost 10% of Morgan Stanley’s 3.5 million wealth management clients while holding a junior position within the company.

Marsh's sentencing is scheduled to take place December 7th. Under nonbinding federal sentencing guidelines, Marsh could face between 30 and 37 months in prison. Under the terms of the plea agreement, Marsh cannot appeal any sentence of 37 months or fewer.