Published on *The National Law Review* https://natlawreview.com

Can a whistleblower disclosure to the SEC about cybersecurity qualify for a SEC whistleblower award?

Article By:

Jason Zuckerman

Dallas Hammer

Yes, a disclosure about cybersecurity that leads to an enforcement action in which the SEC collects one million or more in penalties will qualify for a SEC whistleblower award. A recent enforcement action against Voya Financial Advisors Inc. (VFA), a broker-dealer and investment adviser, demonstrates the SEC's increased commitment to enforcing rules requiring brokers and advisers to safeguard customer information. In particular, VFA is paying $1 million to settle charges that it failed to protect brokerage customer and advisory client information.

VFA's practice was to give its independent contractor representatives, the majority of its workforce, access to customer information through a proprietary web portal that could be accessed remotely from the contractors' personal devices. During a six-day period in April of 2016, unknown persons accessed the web portal by impersonating VFA contractors and calling the technical support line to request password resets. The passwords were reset, and the imposters were given temporary passwords over the phone, giving them access to 5,600 VFA customers' personally identifiable information (PII).

After the breach, VFA failed to address deficiencies in its cybersecurity program, including aspects of the design, implementation, and employee training. And even after one of the advisers alerted VFA that he had not requested a new password, two more advisers were impersonated.

The Safeguards Rule (Rule 30(a) of Regulation S-P codified at 17 C.F.R. § 248.30(a)) requires broker-dealers and investment advisers to have written policies and procedures that address the protection of customer records and information. The policies "must be reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

The Identity Theft Red Flags Rule (Rule 201 of Regulation S-ID (17 C.F.R § 248.201)) requires certain financial institutions and creditors registered with the SEC to create and implement a written Identity Theft Prevention program. "An Identity Theft Prevention Program must include reasonable

policies and procedures to: identify relevant red flags for the covered accounts and incorporate them into the Identity Theft Prevention Program; detect the red flags that have been incorporated into the Identity Theft Prevention Program; respond appropriately to any red flags that are detected pursuant to the Identity Theft Prevention Program; and ensure that the Identity Theft Prevention Program is updated periodically to reflect changes in risks to customers from identity theft."

According to the SEC's order, VFA violated the Safeguards Rule because its policies and procedures to protect customer information and to prevent and respond to cybersecurity incidents were not reasonably designed to meet these objectives. And VFA violated the Identity Theft Red Flags Rule because it did not review and update the Identity Theft Prevention Program in response to changes in risks to its customers or provide adequate training to its employees.

Whistleblower Protections and Incentives for Cybersecurity Whistleblowers

Zuckerman Law has represented cybersecurity whistleblowers in whistleblower retaliation and whistleblower rewards claims, including in Sarbanes-Oxley whistleblower actions. Dallas Hammerhas written extensively about protections for cybersecurity whistleblowers, including the following publications:

- The Rise of Cybersecurity Whistleblowing, NYU Law Compliance & Enforcement Blog (December 2016)
- Cybersecurity Whistleblowing: What Employees at Public Companies Should Know Before Reporting Information Security Concerns, ISSA Journal (June 2016)

Recently the Wall Street Journal quoted Hammer extensively in an article titled Cybersecurity Whistleblowers Are Growing Corporate Challenge. Corporate Crime Reporter interviewed Mr. Hammer about cybersecurity whistleblowing: Dallas Hammer on the Rise of Cybersecurity Whistleblowing. And CSO quoted Mr. Hammer in an article titled Cybersecurity whistleblowers: Get ready for more.

To learn more about the SEC Whistleblower Program, download Zuckerman Law's eBook: SEC Whistleblower Program: Tips from SEC Whistleblower Attorneys to Maximize an SEC Whistleblower Award.

National Law Review, Volume VIII, Number 281