THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 51 No. 12 June 20, 2018

THE FUTURES INDUSTRY AND CYBERSECURITY

The regulatory framework for cybersecurity in the derivatives markets is evolving to meet the growing threat of cyberattacks. The authors describe these regulatory initiatives, focusing on the SEC's recent cybersecurity examinations and the CFTC's first cybersecurity enforcement action. They conclude with key cybersecurity takeaways for derivatives industry organizations.

By William Ridgway, Jonathan Marcus, and Alexander Kasparie *

Cyberattacks on financial institutions and infrastructures have grown more frequent, complex, and sophisticated. And the motivation behind such attacks is shifting from financial gain to disruption, such as through nation-state attacks, which threaten to undermine confidence in the financial system. Recognizing the gravity of these risks, financial regulators have made cybersecurity a priority. Indeed, the CFTC recently joined the growing list of regulators that police this area in bringing its first enforcement action relating to cybersecurity.[1] That action underscores the need for robust oversight of cybersecurity and the ease with which a regulated entity can find itself in the crosshairs of an enforcement action. Given the increasing regulatory scrutiny and sophistication of the threats, futures industry market participants would do well to take a fresh and comprehensive look at their cybersecurity preparedness, governance, internal controls, and defenses.

THE REGULATORY FRAMEWORK

Regulations and interpretive notices from the CFTC, the SEC, and the National Futures Association ("NFA"), the self-regulatory organization for the U.S. derivatives industry, set forth the evolving regulatory framework for cybersecurity in the derivatives markets. Although these regulations focus on different areas, they collectively embody a set of requirements and best practices for market participants to follow.

As a starting point, futures commission merchants and introducing brokers are required to "adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information" under CFTC Regulation 160.30. The NFA's interpretive guidance similarly

[1] CFTC No. 7693-18, 2018 WL 816833 (Feb. 12, 2018).

* *WILLIAM RIDGWAY is a partner, JONATHAN MARCUS is of counsel, and ALEXANDER KASPARIE is an associate at Skadden, Arps, Slate, Meager & Flom, LLP. Their e-mail addresses are william.ridgway@skadden.com, jonathan.marcus@skadden.com,* and *alexander.kasparie@skadden.com*. The views expressed herein are those of the authors and are not necessarily the views of Skadden Arps or its clients.