The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 35237

April 11, 2023

China Releases Cybersecurity and Data Security Rules for Securities and Futures Industry

[35237]

April 11, 2023

TO: ICI Global Members
Chief Information Security Officer Committee
Global Information Security Officer Committee - London
Global Information Security Officer Committee - Tokyo
Global Regulated Funds Committee
Global Regulated Funds Committee - Asia SUBJECTS: Cybersecurity
International/Global
Operations RE: China Releases Cybersecurity and Data Security Rules for Securities and Futures Industry

On February 27, 2023, the China Securities Regulatory Commission (CSRC) finalized a set of cybersecurity and data security regulatory requirements (hereafter "the Administrative Measures") for the securities and futures sectors[1] in response to China's three-pronged regulatory framework on information security, i.e., the Cybersecurity Law (CSL), the Data Security Law (DSL) and the Personal Information Protection Law (PIPL). Fund management companies (FMCs), among other industry players,[2] will be required to comply with the cybersecurity and data security requirements from May 1, 2023.

Notably, compared to the consultation draft,[3] the Administrative Measures strengthen requirements on investors' personal data protection, including their biometric data. The final Administrative Measures also included updated guidance related to data storage, vendor management, and record keeping, particularly as it relates to "important" information systems.[4]

The Administrative Measures did not address cross-border data transfer restrictions, which is a significant issue for global asset managers. Based on ICI Global's discussions with CSRC officials, we understand that the Chinese authorities are working on providing additional guidance and clarifications on these restrictions, but the timeline for such guidance remains uncertain.

NOTABLE CHANGES IN THE FINAL VERSUS DRAFT ADMINISTRATIVE MEASURES

Enhanced Requirements on Personal Data Protection

The Administrative Measures provide additional detail on the regulatory expectations on personal data handling. FMCs should inform investors of the purpose, methods, and scope of personal data processing, as well as personal data protection policies. FMCs may collect only the personal data that is necessary to provide services to investors, and may not collect personal data beyond the stated scope. Where an investor refuses to give consent to the data processing request or withdraws his/her consent, FMCs should not refuse to offer services to such an investor unless the data requested for processing is essential for the services.

In case of providing personal data to a third party, FMCs should obtain separate consent from investors, and additionally inform the investors of categories of processed personal data, retention periods, data protection mechanisms, and the rights and responsibilities of that third party. The Administrative Measures set out further measures that FMCs should implement to secure personal data, for instance, data encryption and masking sensitive personal data. FMCs should not use biometrics as the only tool for authentication. Other authentication methods should be offered, such that investors may choose to reject the processing of their biometric data.

Discretion to Back up Data to Industry Strategic Backup Data Centre

CSRC will build a strategic backup data center for the securities and futures industry, at which the backup and management of industry data will be centralized. CSRC encourages critical information infrastructures (CIIs)[5] in the securities and futures sectors to back up their data to the industry strategic backup data center. Instead of mandating FMCs to submit their data to the strategic backup data center as proposed in the consultation draft, FMCs who are not CIIs have the discretion to decide whether or not to back up their data to the industry strategic backup data center.

New Requirements on Information Technology Vendor Management

The Administrative Measures added that FMCs should establish a robust process for selecting vendors and monitoring the quality of products and services. The vendor contracts should clearly state the duties of both FMCs and the information technology vendors on cybersecurity and data security. FMCs should also ask the information technology vendors to sign non-disclosure agreements. Information technology vendors are obliged to work with CSRC in investigating any cybersecurity incidents triggered by their products or services.

Vendors who provide products or services to FMCs' important information systems are required to file with the CSRC as Information Technology Service Institutions. FMCs should ask the relevant vendors to meet their filing responsibilities.

Refined Requirements on Record Keeping and Backup Frequency

The CSRC refined the scope of record-keeping and data backup requirements, and only the important information systems are subject to these requirements. FMCs should establish local, intra-city, and remote data backup facilities, and back up their important information

systems at least once a day. The retention period of business logs of important information systems is also significantly reduced from 20 years to five years.

FMCs should also conduct stress testing of important information systems at least once a year, and keep a record of stress test reports for at least five years.

Lisa Cheng
Senior Research Analyst
ICI Global

Notes

[1] Administrative Measures for Cybersecurity and Data Security in the Securities and Futures Industry, February 27, 2023, available (in Chinese only) at http://www.csrc.gov.cn/csrc/c101953/c7202800/content.shtml.

[2] The Administrative Measures apply to (i) operators of securities and futures market infrastructure (e.g., securities and futures exchanges, and securities depository and clearing institutions), (ii) securities and futures business institutions (e.g., securities companies, future companies, and fund management companies), and (iii) Information Technology Service Institutions which provide products or services for the important information systems of the securities and futures sectors. See Administrative Measures, supra note 1, at Article 71(5).

[3] The CSRC consulted the draft Administrative Measures in April 2022. See ICI Memorandum [34143], dated May 17, 2022, available at https://www.ici.org/memo34143, Administrative Measures for Cybersecurity Relating to the Securities and Futures Industry (Draft for Comments), April 29, 2022, available (in Chinese only) at http://www.csrc.gov.cn/csrc/c101981/c2381308/content.shtml.

[4] Important information systems refer to systems that are involved in key business functions of the securities and futures sectors, where any disruptions or data leakage may significantly impact the securities and futures market, and investors. See Administrative Measures, supra note 1, at Article 71(5).

[5] CIIs are defined as information infrastructure in the industries of public communication and information service, energy, transportation, water resources, finance, public service, e-government, national defense and military affairs and other important network facilities and information systems, the disruption, disfunction, and data leakage of which may endanger national security, civil livelihood, and public interest. See Regulations for the Security Protection of Critical Information Infrastructure, available (in Chinese only) at: http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm.

Copyright © by the Investment Company Institute. All rights reserved. Information may be abridged and therefore incomplete. Communications from the Institute do not constitute, and should not be considered a substitute for, legal advice.