NORTHCAPITAL

NOTICE TO SERVICE PROVIDERS AND COVERED INSTITUTION CUSTOMERS

Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information

Background. In 2024, the U.S. Securities and Exchange Commission (SEC) adopted amendments to Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information (Regulation S-P) under the Gramm-Leach-Bliley Act (GLBA). Regulation S-P governs the treatment of nonpublic personal information[1] by certain financial institutions. The amendments apply to "covered institutions", including broker-dealers (including funding portals), investment companies, registered investment advisers and transfer agents. The compliance date for larger covered institutions is December 3, 2025.[2]

As amended, Regulation S-P requires covered institutions to adopt and implement written policies and procedures for an incident response program reasonably designed to detect, respond to and recover from unauthorized access to or use of customer information. The program must include procedures for providing notice to affected individuals whose sensitive customer information[3] was, or is reasonably likely to have been, accessed or used without authorization, as soon as practicable but no later than 30 days after becoming aware of such unauthorized access or use, subject to any permitted law enforcement delay.

The incident response program must also include written policies and procedures reasonably designed to require oversight of service providers[4] that have access to customer information, including measures to ensure that service providers: (i) take appropriate measures designed to protect against unauthorized access or use of customer information; and (ii) notify the covered institution as soon as possible, but no later than 72 hours after becoming aware that a breach of a customer information system maintained by the service provider has occurred resulting in unauthorized access to or use of customer information.

Notice to Service Providers to North Capital.[5] Service providers are a critical component of North Capital's incident response program. If you are a service provider to North Capital, you are required to:

- ⇒ Maintain appropriate safeguards designed to protect against unauthorized access to or use of customer information;
- ⇒ Notify North Capital as soon as possible, but not later than 72 hours after becoming aware that a breach of a customer information system maintained by you has occurred resulting in unauthorized access to or use of customer information;
- ⇒ Promptly coordinate with North Capital to determine the nature and scope of the incident, including what systems and customer information were or are reasonably likely to have been accessed or used;
- ⇒ Preserve relevant records and cooperate fully in any investigation relating to the incident; and
- ⇒ Assist North Capital in complying with its obligations to provide notice to affected individuals under Regulation S-P, including within the applicable 30-day period following North Capital's awareness that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred, unless a permitted law enforcement delay applies.

Notice to North Capital Covered Institution Customers. As a service provider to covered institutions, North Capital recognizes its responsibility to support its covered institution customers' incident response programs. If you are a covered institution customer of North Capital, and North Capital receives, maintains, processes or is otherwise permitted access to customer information in connection with providing services to you, North Capital will undertake to:

---

[1] "Nonpublic personal information" means: (i) personally identifiable financial information; and (ii) any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available information. Nonpublic personal information does not include publicly available information, except as included in a list, description, or other grouping of consumers that is derived using personally identifiable financial information that is not publicly available information.

[2] "Larger" covered institutions include broker-dealers that do not qualify as small entities under the SEC's definition (i.e., broker-dealers that do not meet all of the small entity criteria, including having total capital of less than $500,000 as of the relevant fiscal year-end measurement date, not being affiliated with any person that is not a small entity and not being a clearing broker-dealer), and registered investment advisers with $1.5 billion or more in assets under management. The compliance date for smaller covered institutions is June 3, 2026.

[3] "Sensitive customer information" means any component of customer information, alone or in conjunction with any other information, the unauthorized access to or use of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. Sensitive customer information includes, but is not limited to, Social Security numbers, driver's license numbers, passport numbers, military identification numbers, employer or taxpayer identification numbers, financial account numbers (including credit or debit card numbers), biometric records, security codes, access codes, passwords or any other information that could be used to access a customer's account or to authenticate an individual's identity.

[4] "Service provider" means any person or entity that receives, maintains, processes or otherwise is permitted access to customer information through its provision of services directly to a covered institution.

[5] "North Capital" refers to, as applicable, North Capital Investment Technology, Inc., a financial technology corporation, and its subsidiaries North Capital Private Securities Corporation and North Capital Agency Brokerage, LLC, registered broker-dealers regulated by the SEC and the Financial Industry Regulatory Authority, Inc., North Capital, Inc., a registered investment advisor regulated by the SEC and a commodities trading advisor regulated by the Commodity Futures Trading Commission, North Capital Trust Company, a South Dakota trust corporation, North Capital Token Services, LLC, a provider of tokenization services, and North Capital Administrator Services Inc.

- ⇒ Maintain appropriate safeguards designed to protect against unauthorized access to or use of customer information;
- ⇒ Notify the covered institution customer as soon as possible, but not later than 72 hours after becoming aware that a breach of a customer information system maintained by North Capital has occurred resulting in unauthorized access to or use of customer information;
- ⇒ Promptly coordinate with the covered institution customer to determine the nature and scope of the incident, including what systems and customer information were or are reasonably likely to have been accessed or used;
- ⇒ Preserve relevant records and cooperate fully in any investigation relating to the incident; and
- ⇒ Assist the covered institution customer in complying with its obligations under Regulation S-P to provide notice to affected individuals, including within the applicable 30-day period following the covered institution's awareness that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred, unless a permitted law enforcement delay applies.

North Capital has documented these commitments in its internal incident response program and, as applicable, seeks confirmation of corresponding commitments from its service providers pursuant to its vendor risk management and assessment process. In further support of its commitment to information security and data privacy, North Capital's disclosures are available here, including its Commitment to Privacy and Notice at Collection and Business Continuity Planning Disclosure Statement.

North Capital undergoes an annual SOC 2 Type II examination conducted by an independent licensed CPA firm. The examination evaluates the suitability of the design and the operating effectiveness of North Capital's controls relevant to the applicable AICPA Trust Services Criteria over a specified examination period, including controls related to its information security program and supporting policies and procedures. North Capital's controls are designed in alignment with the AICPA Trust Services Criteria applicable to the scope of the examination. North Capital's SOC 3 report is a general-use report derived from the SOC 2 examination. It provides a high-level summary of the independent auditor's opinion regarding the effectiveness of North Capital's controls during the examination period and is intended for public distribution. The SOC 3 report does not include detailed descriptions of controls, test procedures or results. The SOC 3 report is available here for informational purposes.

* * *