CTA and CQ Plans Administrator and Processor Confidential Information Policy

9/1/2020

Copyright Information

Revision History

Date	Author	Changes	Approval
2020.09.01	L. Bui	Initial version of policy.	E. King

1. Background 5
2. Purpose and Scope of the Policy 5
2.1 Purpose of the Policy 5
2.2 Information Covered by the Policy 6
2.3 Classification of Information 7
2.4 Personnel Covered by the Policy 8
3. Procedures to Maintain Confidentiality 9
3.1 Disclosure and Use of Plan Information 9
3.1.1 Disclosure to Other Designated Personnel that are Third Parties 9
3.1.2 Disclosure of Restricted Information to the Operating Committee 9
3.1.3 Access to CTA Plan Web Portal 10
3.1.4 Use of Plan Information 10
3.2 Aggregation, Redaction, and Anonymization of Plan Information 10
3.3 PDP Information Barrier 11
3.3.1 Prohibition on Crossing the Information Barrier 11
3.3.2 Operational Separation 11
3.3.3 Meetings 11
3.4 CTA Plan Data Information Barrier 12
3.5 Security Measures 12
3.6 Third-Party Vendor Agreements 13
4. Reporting Requirements 13
5. Updates to the Policy 14

1. Background

Under the CTA and CQ Plans (each a "Plan" and, collectively, the "Plans"), New York Stock Exchange LLC ("NYSE") is the network administrator for CTA and CQ Network A,[1] and NYSE American LLC ("NYSE American") is the network administrator for CTA and CQ Network B. Under Section IX(f) of the CTA Plan and Section VII(f) of the CQ Plan, NYSE performs the administrator functions for both Network A and Network B (the "Administrator"). Under Section V(a) of the CTA Plan and Section V(a) of the CQ Plan, the Securities Industry Automation Corporation ("SIAC") is designated as the securities information processor to the Plans (the "Processor"). SIAC has entered into a Processor Agreement with each of the Participants.

Under the Plans, the Administrator is required to perform certain administrative functions on behalf of the Plans, including recordkeeping, billing, distribution of revenue, preparation of financial reports, and negotiation of third-party contracts on behalf of the Plans.

Under the Plans and the Processor Agreements with Participants, the Processor performs certain processing functions on behalf of the Plans, including: (i) collection of quotation information and transaction reports from Participants, (ii) consolidation and processing of such information, and (iii) dissemination of such information to vendors and subscribers.

The Administrator and Processor are affiliated with certain of the Plan Participants that are required under Rule 608(c) of Regulation NMS to comply with the terms of the Plans. Neither the Administrator nor the Processor are required under the Securities Exchange Act of 1934 or Securities and Exchange Commission rules to comply with the terms of the Plans and are instead subject to administrative oversight of the Operating Committee of the Plans. The Plans require the Administrator and Processor to establish a written confidential information policy (the "Policy") that provides for the protection of information under their control and the control of their Agents, including policies and procedures that provide systemic controls for classifying, declassifying, redacting, aggregating, anonymizing, and safeguarding information, that is in addition to, and not less than, the protection afforded in the Confidentiality Policy of the Plans set forth in Exhibit G to the CTA Plan and Exhibit F to the CQ Plan (the "Confidentiality Policy").

The Policy is subject to review and approval by the Plans' Operating Committees, will be publicly posted, and be made available to the Operating Committee for review and approval every two years thereafter or when changes are made, whichever is sooner.

2. Purpose and Scope of the Policy

2.1 Purpose of the Policy

The purpose of this Policy is to set forth the policies and procedures for the Administrator and Processor to protect confidential plan information. These policies and procedures include information barriers

[1] Unless otherwise defined, capitalized terms used herein have the meanings set forth in the Plans.

established and described below in this Policy, as well as other confidentiality and information security requirements.

2.2 Information Covered by the Policy

Unless otherwise specified, the requirements under this Policy apply to the treatment, use of, access to, and disclosure of Plan Information, Administrator Information, and Processor Information.

"Administrator Information" includes all information necessary for the Administrator to perform its role on behalf of the Plans and includes financial reporting, recordkeeping, revenue, contracting, and other customer-specific or individual-specific financial or other sensitive information relating to the Plans.

"Processor Information" includes all information necessary for the Processor to perform its role on behalf of the Plans and includes data collected, consolidated, and disseminated by the Processor, as well as Participant-specific information related to such collection, consolidation, and dissemination.

"Plan Information" refers to both Administrator Information and Processor Information. Except as specifically noted below, any information obtained in connection with the provision of services as Processor or Administrator for the Plans is assumed to be Plan Information.

Without limiting the foregoing, Plan Information specifically includes:

(i) transaction reports, quotation information, and related information provided by Participants to the Processor or collected, consolidated or disseminated by the Processor, including CQ/CTA data prior to its dissemination to customers;

(ii) financial, operational, technical, or other information about customers, including but not limited to lists of customers, customer contact information, demographics pertaining to customers, billing data and reports from customers concerning usage such as subscriber counts, and personally identifiable information;

(iii) information about the identity or activities of, contracts entered into or negotiated by, or pricing for CQ/CTA data obtained by, customers (including, for example, vendor agreements, system descriptions, data feed or other request forms, invoices, and approval letters);

(iv) information obtained or calculated by the Processor or the Administrator in connection with its services on behalf of the Plan, including but not limited to revenue forecasting data, compliance information and reports or other analytics generated for the Participants; and

(v) financial, operational, technical, or other information about Participants, including but not limited to capacity planning information and information relating to each individual Participant's proportional share of expenses and revenues in accordance with the Plan and the Revenue Allocation System formulas.

Plan Information does not include information that:[2]

(i) is not Restricted Information, Highly Confidential Information, or Confidential Information (as defined below) or is otherwise publicly available;

(ii) was created by the Administrator or Processor without use of or reference to any Plan Information; and

(iii) was lawfully received free of restriction from another source with the right to furnish such information, including data included in the CQ/CTA data after it has been disseminated to Customers.

2.3 Classification of Information

The Plans require the Administrator to classify Plan Information. The four categories of information are (1) Restricted Information; (2) Highly Confidential Information; (3) Confidential Information; and (4) Public Information, which are defined in the Confidentiality Policy as follows:

(1) Restricted Information. Highly sensitive customer-specific financial information, customer-specific audit information, other customer financial information, and Personal Identifiable Information.

(2) Highly Confidential Information. Any highly sensitive Participant-specific, customer-specific, individual-specific, or otherwise sensitive information relating to the Operating Committee, Participants, or customers that is not otherwise Restricted Information. Highly Confidential Information includes: a Participant's contract negotiations with the Processor or Administrator; personnel matters; information concerning the intellectual property of Participants or customers; and any document subject to the Attorney-Client Privilege or Work Product Doctrine.

(3) Confidential Information. Except as otherwise covered by one of the other categories, (i) any non-public data or information designated as Confidential by a majority vote of the Operating Committee; (ii) any document generated by a Participant or Advisor and designated by that Participant or Advisor as Confidential; and (iii) the individual views and statements of Covered Persons and SEC staff disclosed during a meeting of the Operating Committee or any subcommittees thereunder.

(4) Public Information. Public information is (i) any information that is not either Restricted Information or Highly Confidential Information or that has not been designated as Confidential Information; (ii) any confidential information that has been approved by the Operating Committee for release to the public; (iii) the duly approved minutes of the Operating Committee and any subcommittee thereof with detail sufficient to inform the public on matters under discussion and the views expressed thereon (without attribution); (iv) Plan subscriber and performance metrics; (v) Processor transmission metrics; and (vi) any information that is

[2] While the information listed is not Plan Information, other information security policies that the Administrator and Processor are subject to may still apply.

otherwise publicly available, except for information made public as a result of a violation of the Confidentiality Policy or any applicable law or regulation. Public Information includes any topic discussed during a meeting of the Operating Committee, an outcome of a topic discussed, or a Final Decision of the Operating Committee, as defined below.

The Administrator posts documents to the Plans' Web Portal (Diligent). Prior to posting any document to the Web Portal or otherwise sharing any document with the Operating Committee or any of its subcommittees, the Administrator will classify and label the document with one of the above categories. The Administrator will review the document to determine the category of information it contains and label it accordingly:

(1) For documents that contain Restricted Information, the Administrator will add the label "Restricted Information." Documents containing Restricted Information will not be posted to the Plans' Web Portal.
(2) For documents that contain Highly Confidential Information, the Administrator will add the label "Highly Confidential Information." Documents containing Highly Confidential Information may only be posted to the Executive Session portion of the Plans' Web Portal.
(3) For documents that contain Confidential Information, the Administrator will add the label "Confidential Information." Documents containing Confidential Information may be posted to the General Session portion of the Plans' Web Portal.

2.4 Personnel Covered by the Policy

This Policy applies to any individuals who perform functions for, or on behalf of, the Administrator or Processor, including: (i) employees of the Administrator and Processor, (ii) employees of an affiliate of the Administrator or Processor, and (iii) third-party attorneys, auditors, advisors, accountants, contractors, subcontractors, and other agents. Individuals covered by the Policy fall into one of the following groups based on their responsibilities and activities:

(1) Designated Administrator Personnel support the functions performed by the Administrator and have access to Plan Information. Designated Administrator Personnel functions include recordkeeping, billing, distribution of revenue, preparation of financial reports, and negotiation of third-party contracts. The Administrator will, in consultation with internal legal counsel, maintain a current list of all Designated Administrator Personnel, who will be required annually to certify that they have read and will abide by this Policy as well as the Confidentiality Policy.

(2) Designated Processor Personnel support the functions that the Processor performs, as described above, and have access to Plan Information. The Processor will, in consultation with internal legal counsel, maintain a current list of all Designated Processor Personnel, who will be required annually to certify that they have read and will abide by this Policy as well as the Confidentiality Policy.

(3) PDP Personnel are individuals whose job functions include marketing and/or selling proprietary data products ("PDPs") on behalf of NYSE, NYSE American, or their affiliated national securities exchanges and will not be permitted to access Plan Information. The NYSE will, in consultation with internal legal counsel, maintain a current list of all PDP Personnel and provide that list to

the Administrator. PDP Personnel will be required annually to certify that they have read and will abide by this Policy as well as the Confidentiality Policy.

(4) Other Designated Personnel are individuals who are not Designated Administrator Personnel, Designated Processor Personnel, or PDP Personnel, but who perform functions for, or on behalf of, the Administrator or Processor. Other Designated Personnel will be designated by the Administrator and Processor, in consultation with internal legal counsel and other appropriate managers, and will have access to Plan Information. Individuals in this group may include those that provide compliance, legal, technology, billing, internal audit, tax, and collections services in support of the Administrator and Processor functions, including third-party providers of such services. External accounting firms that perform annual financial audit or tax services and outside legal counsel that provide legal services to the Administrator or Processor are included in this group. Other Designated Personnel will be required annually to certify that they have read and will abide by this Policy as well as the Confidentiality Policy.

3. Procedures to Maintain Confidentiality

Individuals with access to Plan Information must treat that information as confidential at all times.

3.1 Disclosure and Use of Plan Information

3.1.1 Disclosure to Other Designated Personnel that are Third Parties

In addition to affirming that they have read and will comply with the terms of this Policy, Other Designated Personnel that are third-party service providers, such as external accounting firms and outside legal counsel, will not be provided Restricted Information, Highly Confidential Information, or Confidential Information, as necessary for such third-party service providers to provide services on behalf of the Plans, until a third-party service provider has completed its subcontractor/service provider disclosure form as required by the Conflicts of Interests provisions set forth in Section IV(f) of the CTA Plan and Section IV(e) of the CQ Plan (the "Conflicts of Interests Policy").

3.1.2 Disclosure of Restricted Information to the Operating Committee

Pursuant to the Confidentiality Policy, the Administrator and Processor are required to keep Restricted Information in confidence. Restricted Information may not be disclosed to the Plans' Operating Committees or any subcommittees thereof.

Should the need arise to share Restricted Information with the Plans' Operating Committee, the Administrator will first anonymize the information by redacting the customer's name and any other information that may lead to the identification of the customer. Where such information has been redacted, any materials should be labeled as Highly Confidential.

In order to share Restricted Information without redacting the customer's name, the Administrator must first determine that disclosure of the customer's identity is necessary to obtain input or feedback from the Operating Committee or a subcommittee thereof about a matter of importance to the Plan(s). Such

instances may include audit issues that require the Operating Committee to authorize legal action. In such instances, any materials should be labeled as Highly Confidential.

In the event the Administrator is aware of any willful, reckless, or grossly negligent conduct of a customer, the Administrator may share such information with the other Administrator or with the SEC Staff upon a majority vote of the Operating Committee in Executive Session. When requesting Operating Committee approval, the Administrator shall not disclose the identity of the party or parties involved and shall remove any other information that may lead to the identification of such parties.

3.1.3 Access to CTA Plan Web Portal

The Administrator is responsible for ensuring that only authorized Covered Persons, as defined in the Confidentiality Policy, have access to the relevant portions of the Plan's Web Portal (Diligent). Access should not be granted unless the Covered Person has affirmed in writing that they will comply with the Confidentiality Policy and, if applicable, the relevant Disclosure Form has been submitted as required by the Conflicts of Interest Policy. The authorized Covered Persons who may have access to the General Session portion of the Plans' Web Portal are the Participants' Representatives and advisors/observers, Advisory Committee Members, SEC Staff, and the Plans' legal counsel. The authorized Covered Persons who may have access to the Executive Session portion of the Plans' Web Portal are the Participant Representatives, SEC Staff, and the Plans' legal counsel. Recused individuals may not have access to the Executive Session portion of the Plans' Web Portal. The Administrator shall review the Plans' Web Portal access on a periodic basis to ensure that only authorized Covered Persons have portal access to Plan materials.

3.1.4 Use of Plan Information

Individuals that have access to Plan Information are prohibited from making use of such information for any purpose other than in connection with the provision of Administrator and Processor services to the Plans.

3.2 Aggregation, Redaction, and Anonymization of Plan Information

When the Administrator compiles Plan Information pertaining to multiple customers to be shared with the Operating Committee or a subcommittee or posted publicly, it will aggregate such information by expressing in summary form individual customer data. Specifically, the Administrator will:

(1) Identify the underlying data points to be collected for each individual customer;
(2) Collect the relevant data for each customer from the database system(s) containing such data;
(3) Build the aggregated values by summarizing the underlying data points pertaining to each customer; and
(4) Transfer the aggregated values to a document that does not associate any individual customer with that customer's information.

The Administrator may also protect Plan Information through redaction and anonymization. If a customer's financial information needs to be shared with the Operating Committee or a subcommittee, the customer's name and any other information that could lead to the identification of the customer will be redacted and anonymized. Before sharing such information, the Administrator will remove

identifiers such as customer names and replace them with pseudonyms (e.g., substitute “Firm 1” or “Firm A” for the customer’s name).

3.3 PDP Information Barrier

As described above, NYSE is the Administrator for the Plans. Separately, NYSE and other securities exchange affiliates of the Administrator offer PDPs.

In addition to the restrictions on the disclosure and use of Plan Information as described above, this Policy establishes an information barrier designed to prevent the disclosure of Plan Information to individuals involved in marketing or selling PDPs.

3.3.1 Prohibition on Crossing the Information Barrier

This Policy establishes a wall between Designated Administrator Personnel, Designated Processor Personnel, and Other Designated Personnel on one side and any other individuals, including PDP Personnel, on the other. The first three groups are deemed to be “behind the wall” and are presumed to be in possession of Plan Information. Such Individuals may not share or disclose any Plan Information with any individuals who are not Designated Administrator Personnel, Designated Processor Personnel, or Other Designated Personnel. Designated Administrator Personnel, Designated Processor Personnel, and Other Designated Personnel are not prohibited from having access to PDP information and may provide services to PDP, provided such services are unrelated to the marketing and selling of PDP products.

3.3.2 Operational Separation

To prevent the inadvertent disclosure of Plan Information, Designated Administrator Personnel, Designated Processor Personnel, and Other Designated Personnel in possession of Plan Information are prohibited from maintaining or leaving such information in shared spaces that are not subject to access requirements. For example, physical files containing Plan Information should not be maintained in a shared location unless restricted to Designated Administrator Personnel, Designated Processor Personnel, and Other Designated Personnel permitted to access such files. All such individuals are also required to comply with other information security policies applicable to the Administrator or Processor.

In addition, the Administrator and Processor have implemented security measures designed to prevent unauthorized use or disclosure of Plan Information. These security measures include technological separation and access requirements to prevent access to Plan Information by anyone other than Designated Administrator Personnel, Designated Processor Personnel, or Other Designated Personnel, as applicable. For more information on these security measures, see Section 3.5 below.

3.3.3 Meetings

In certain circumstances, Designated Administrator Personnel, Designated Processor Personnel, and Other Designated Personnel, as well as senior management, may need to attend meetings that also involve the participation of PDP Personnel. Designated Administrator Personnel, Designated Processor Personnel, and Other Designated Personnel, as well as senior management, should take care not to

share any Plan Information in meetings where PDP Personnel may be present. PDP Personnel are not permitted to attend meetings where Plan Information may be discussed.

3.4 CTA Plan Data Information Barrier

Individual Participants of the Plans provide transaction reports, quotation information, and related information to the Processor for collection, consolidation, and dissemination ("CTA Plan Data"). Only Designated Processor Personnel and Other Designated Personnel of the Processor are permitted to access CTA Plan Data.

The Processor has implemented security measures designed to prevent unauthorized access to CTA Plan Data. These security measures include technological separation and access requirements to prevent the sharing of CTA Plan Data by Designated Processor Personnel and Other Designated Personnel of the Processor. For more information on these security measures, see Section 3.5 below.

3.5 Security Measures

Plan Information is maintained in systems that use security measures designed to prevent access by or disclosure to anyone other than Designated Administrator Personnel, Designated Processor Personnel, and Other Designated Personnel. These security measures include access restrictions designed to implement the PDP information barrier described in Section 3.3 and the CTA Plan Data information barrier described in Section 3.4.

The security measures include the following:

(1) Plan Information that includes Restricted Information and Highly Confidential Information is stored in database systems that contain data such as customer information, reporting detail, and supporting documentation for both CTA and PDPs. The systems include client inventory, billing information, Vendor Reporting, Data Feed and Subscriber Approval Request processes, Account and Contact Management, and Company Financials along with Reports and Utilities for the Market Data business. Plan Information in these systems is segregated and only Designated Administrator Personnel, Designated Processor Personnel, and Other Designated Personnel with responsibilities for finance functions on behalf of the Plans are provided access to Plan Information in these systems. Accordingly, only such designated Personnel may be assigned ID/Passwords[3] to access the Plan Information on these systems.

(2) Each user accessing Plan Information in these systems must be assigned his or her own unique ID/Password, which may not be shared. Individuals not assigned such ID/Passwords will not have access to these systems.

(3) The Administrator and Processor will determine which Designated Administrator Personnel, Designated Processor Personnel, and Other Designated Personnel may be granted access to these systems and have the ability to add or remove an individual's access to the database

[3] ID/Passwords will also be subject to other information security policies applicable to the Administrator and Processor, including requirements relating to the resetting or reauthentication of passwords.

systems that store Plan Information as needed. ID/Passwords follow enrollment and disenrollment standards designed to restrict access to Plan Information based on the principle of least privilege, and access will be promptly revoked for any individuals who no longer have a need for such access. Periodic authentication reports are generated to review individuals who are entitled to access these systems.

(4) Downstream systems that perform functions for, or on behalf of, the Administrator or Processor will also follow enrollment and disenrollment standards designed to restrict access to Plan Information based on the principle of least privilege. Access to Plan Information is only granted to downstream systems in connection with functions performed for, or on behalf of, the Administrator or Processor, and access will be promptly revoked for any downstream systems that no longer have a need for such access.

(5) Physical records related to CTA customers are maintained by Designated Administrator Personnel in archives. Access to those records is similarly restricted only to Designated Administrator Personnel, Designated Processor Personnel, and Other Designated Personnel only to provide services on behalf of the Plans.

3.6 Third-Party Vendor Agreements

Third-party vendor agreements managed by Designated Administrator Personnel on behalf of the Participants are stored in a shared department drive that is subject to the access controls and other security measures described in Section 3.5. Access to the shared drive containing the vendor agreements is restricted to Designated Administrator Personnel only, who have a need to know such information in connection with performing services for the Plan.

4. Reporting Requirements

If any individual subject to this Policy has reason to believe that Plan Information has been disclosed in a manner inconsistent with this Policy, such individual may report such potential unauthorized disclosure to the Chair of the Operating Committee.

If any individual subject to this Policy has reason to believe that there has been any violation of this Policy, including that a system grants PDP Personnel or other individuals that are not Designated Administrator Personnel, Designated Processor Personnel, or Other Designated Personnel access to Plan Information, such individual must report such violation to internal legal counsel.

If any individual subject to this Policy inadvertently includes Plan Information in an email chain forwarded to anyone other than the individuals identified in the policy permitted to access such information, such individual must promptly inform internal legal counsel and instruct the individual(s) that received such information to delete the email. The following text should be emailed to the recipient, with a copy to internal legal counsel:

The email message inadvertently sent to you on [date/time] contained confidential CQ/CTA Plan information. Please delete the email from your Inbox, your email trash folder, and any other electronic

folder that may hold it, and shred any paper copies that may have been created from that communication. Please confirm that all of these steps have been followed in a response to this email.

5. Updates to the Policy

This Policy may be updated from time to time, including to reflect any modifications to the confidentiality requirements of the Administrator or Processor due to a policy change by the Plans' Operating Committee. If the Policy is updated, all Designated Administrator Personnel, Designated Processor Personnel, PDP Personnel, and Other Designated Personnel will be notified of the update.

This Policy shall be presented to the Operating Committee for review every two years or when changes are made, whichever is sooner.

* * * * *

I affirm that I have reviewed this Policy and will abide by its terms.

By: _____

Print Name:

Title: