Privacy Impact Assessment
for
Order Book On Demand (OBOD)

6/11/2020

System/Business Owner

Ed Wehner
Associate Director, Data Engineering and Processing
Office of Data and Technology

Reviewing Official
Charles Cutshall
Chief Privacy Officer
Commodity Futures Trading Commission

I. SYSTEM OVERVIEW

1) Describe the purpose of the system/collection:

Order Book on Demand (OBOD) is a cloud hosted system that will allow for the storage, loading, and analysis of data from the Chicago Mercantile Exchange (CME Group), a company comprised of four Designated Contract Markets (DCMs). Through OBOD, CFTC staff will have routine, repeatable access to three CME Group data sets that together comprise the Order Book Data – the Trade Capture Report (TCR), Order Entry, and Market by Order (MBO).

The TCR data represent details of each executed transaction at the exchange and contain reference codes which identify certain market participants, including the tag 50, which identifies the operator who keyed in the order. The Order Entry data represent the order messages that were processed by the exchange and contain information that identifies every trader that is active in the futures and options markets, such as the identity of the trader who is participating in the negotiation for a futures or options contract. The MBO data represent the state of the market as the order messages were processed by the exchange, and contain the order quantities and the priority of orders in the queue for fulfillment at each given price level for the contract. MBO data are not linked or linkable to an individual trader. The data sets are collected by CME Group and provided to the CFTC in accordance with Part 16 of the Commodity Exchange Act (CEA).

The Division of Enforcement (DOE), Division of Market Oversight (DMO), Office of Chief Economist (OCE), and the Division of Clearing and Risk (DCR) all rely on this data to perform their responsibilities and to fulfill the CFTC's obligations under the CEA.

2) Provide a data map or model illustrating how information is structured or is processed by the system throughout its life cycle. Include a brief description of the data flows.

1. Within the Amazon Web Service (AWS) cloud, daily feeds push CME Group data directly into the OBOD system where it is validated and prepared for analysis.

2. Using a native AWS workspace client within CFTC's AWS Cloud environment, CFTC staff can access a variety of tools to perform research as well as market analysis and compliance activities. These tools give CFTC staff access to machine learning that is used to perform proactive trend analysis.

3. Analytic connections between CFTC's on-premises environment and CFTC's AWS cloud environment can be established using an on-premises AWS workspaces client, Statistical Analysis Software (SAS), and a teletypewriter (TTY) emulator. Access to the CFTC's AWS cloud environment is only available through a connection that originates from the CFTC's on-premises network.

4. If necessary, data can be exported from CFTC's AWS cloud environment and stored in secure storage on the CFTC's on-premise environment.

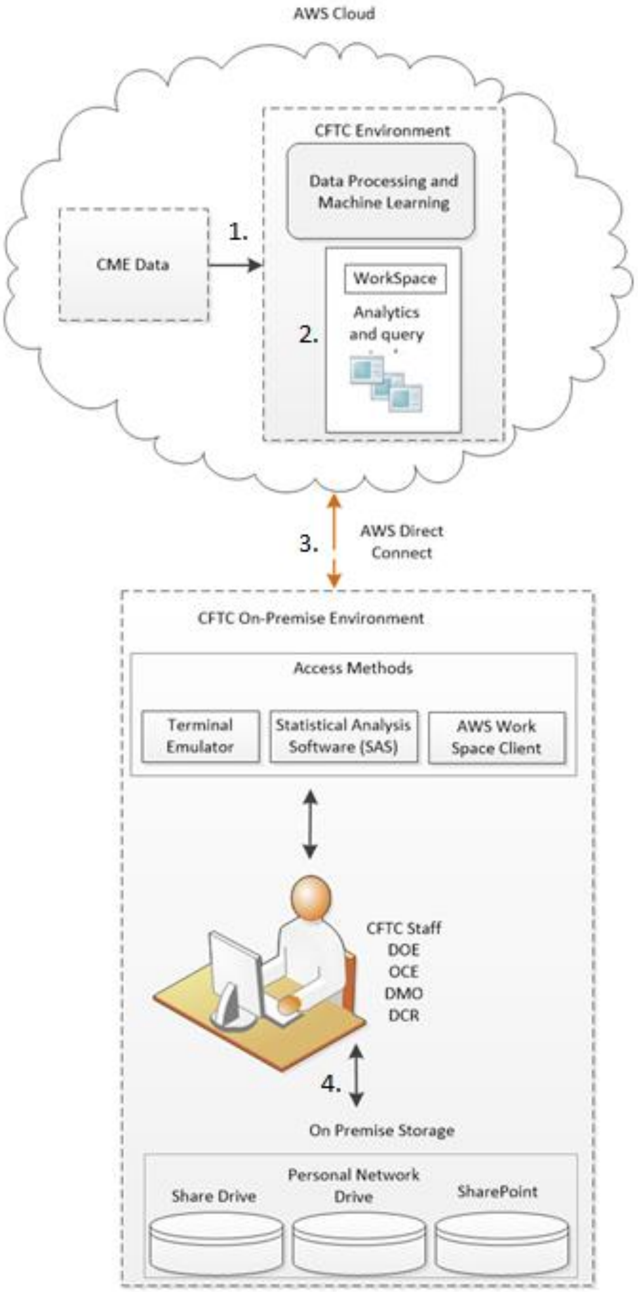

Figure 1 - File Flow Architecture - depicting how data flows through the environment

II. AUTHORITY AND PURPOSE

1) What is the legal authority to collect, use, maintain, and share information in the system?

The CFTC has authority to collect this information under the Commodity Exchange Act (CEA) Part 16.02 – Daily Trade and Supporting Data Reports.

III. INFORMATION TYPES

1) What information will be collected, maintained, used, and/or disseminated?

Identifying Numbers	
☐ Social Security Number	☐ Truncated or Partial Social Security Number
☐ Driver's License Number	☐ License Plate Number
☐ Patient ID Number	☐ File/Case ID Number
☐ Student ID Number	☐ Health Plan Beneficiary Number
☐ Passport Number	☐ Federal Student Aid Number
☐ Employee Identification Number	☐ Taxpayer Identification Number
☐ Professional License Number	☐ Legal Entity Identifier
☐ Credit/Debit Card Number	☐ National Futures Association ID
☐ Personal Bank Account Number	☒ Other ID if it can be traced back to an individual
☐ Personal Device Identifiers or Serial Numbers	TCR data that may be linked to an individual includes: executing broker, clearing member, opposite broker and clearing member, customer type indicator, and trading account numbers.
Contact Information	
☐ Personal Mobile Number	☐ Business Phone Number
☐ Personal E-mail Address	☐ Business E-mail Address
☐ Home Phone Number	☐ Personal or Business Fax Number
☐ Home Mailing Address	☐ Business Mailing Address
Sole Proprietors	
☐ Business Taxpayer Identification Number	☐ Business Mailing Address
☐ Business Credit Card Number	☐ Business Phone or Fax Number
☐ Business Bank Account Number	☐ Business Mobile Numbers
☐ Business Device identifiers or Serial Numbers	
Biographical Information	
☒ Name	☐ Gender
☐ Date of Birth	☐ City or County of Birth
☐ Country of Birth	☐ Zip Code
☐ Citizenship	☐ Military Service Information
☐ Spouse Information	☐ Academic Transcript
☐ Group/Org. Membership	☐ Resume or Curriculum Vitae
☐ Location Data (e.g., GPS)	☐ Nationality

☐ Employment Information	☐ Marital Status
☐ Mother’s Maiden Name	☐ Children Information
Biometrics/Distinguishing Features/Characteristics	
☐ Fingerprints	☐ Height
☐ Retina/Iris Scans	☐ Voice/Audio Recording
☐ Hair Color	☐ Eye Color
☐ Video Recording	☐ Photos
☐ Weight	☐ Signatures
Active Directory/Device Information	
☐ IP Address	☐ MAC Address
☐ CFTC Asset Number	☐ Device Identifiers or Serial Numbers
☐ User Name	

IV. COLLECTING INFORMATION

1) How is the information in this system collected?

The information is collected by the CME Group and provided to the CFTC through an automated daily feed.

V. INFORMATION USE

1) Will information in the system be retrieved using one or more of the data elements listed in Section III?

In the course of a forensic investigation, the information within the OBOD system is retrieved using a trader’s identifiers.

2) If the information in the system is retrieved using one or more of the identifiers, what CFTC System of Records Notice (SORN) covers the information?

Information in this system is covered by CFTC-10, *Investigatory Records* (76 FR 5973) and CFTC-15, *Enterprise Surveillance, Oversight & Risk Monitoring System* (77 FR 58814).

VI. ACCESS AND SHARING

1) With which internal CFTC Offices or Divisions is the information shared? For each Office or Division, what information is shared and for what purpose?

DOE, OCE, DMO and DCR all have access to the information to perform their functions. The information may be shared internally among these offices or divisions where collaboration is required to perform their responsibilities, including:

- DOE requires the data to perform market surveillance in support of investigations.

- OCE requires the data for market analysis and to understand market liquidity in the futures and options markets.

- DMO requires the data to perform market analysis, compliance, and gain an understanding of market performance.

- DCR requires the data to understand market risk.

2) How is the information shared internally?

The information hosted in the CFTC's AWS cloud environment is available only to those users who have been granted access. Access is granted on a case by case basis to CFTC users who have a need to access the information in the performance of their official duties.

In limited circumstances it may be necessary for individuals to download extracts of the data sets to the CFTC's on-premises network. Data is shared electronically via email or through the use of secured network drives with access controls. That data may be shared with peers within the CFTC who have a need to know in the performance of their official duties.

3) With which external organization(s) is the information shared?

The information may be shared with external parties, including other federal, state, foreign regulators per an MOU, Access Grant, or Non-Disclosure Agreement. For example, the information may be shared with the Department of Justice (DOJ) for an active investigation, or with opposing counsel for an active litigation case. The information may also be shared with external subject matter expert consultants in support of an investigation.

4) How is the information shared externally?

External parties do not have direct access to the information in the OBOD system. Information sharing is performed on a case by case basis and is shared electronically either through email or secured electronic transfer mechanisms such as SFTP. All sensitive information is encrypted and its distribution is limited to those who have a need to know. In all cases, the sharing of information must be supported by one of the following three documents:

- Memorandum of Understanding
- Access Grant
- Non-Disclosure Agreement

VII. TRANSPARENCY

1) How are individuals notified as to how their information will be collected, used, and/or shared within this system?

   Information is shared with the CFTC by the CME Group as a result of market participant's activity in the market. This PIA and the applicable SORNs identified in section V above provide notice of the CFTC's collection of this information. CME Group also provides notice in it privacy policy that they share information they collect with the CFTC.

2) Is a SORN required? If so, explain how the use of the information in this system is limited to the use specified in the SORN?

   A SORN is required. Information in this system is covered by CFTC-10, *Investigatory Records* (76 FR 5973) and CFTC-15, *Enterprise Surveillance, Oversight & Risk Monitoring System* (77 FR 58814). The use of this information is limited to the uses specified in the SORNs by controlling access and use of the information through technical as well as procedural and policy controls to those who have a need to know.

VIII. INDIVIDUAL PARTICIPATION

1) Is the information collected directly from the individual?

   No, CFTC collects the information from CME Group. CME Group collects the information from the individuals.

2) Is the collection mandatory or voluntary? If voluntary, what opportunities do the individuals have to decline to provide information?

   The collection of this information is mandatory and is required as a result of market participation.

3) Do individuals have an opportunity to consent to a particular use of the information? If so, how do they provide consent for a particular use?

   No, individuals do not have an opportunity to consent to a particular use of the information. The collection and use of the information is required as a result of market participation.

IX. DATA MINIMIZATION

1) What steps were taken to minimize the collection of PII in the system?

   During the requirements phase the different business users of the data reviewed the data available from the exchanges and made decisions about what data would be needed to accomplish their specific tasks. Only the data identified by the business users is ingested into the system. In addition, the environment is structured to encourage usage without causing data sprawl (whereby multiple copies of the data would be created).

X. DATA QUALITY AND INTEGRITY

1) How is data quality ensured throughout the information lifecycle and business processes associated with the use of the information?
☒ Cross referencing data entries with other systems
☐ Third party data verification
☐ Data taken directly from individuals
☐ Character limits on text submissions
☐ Numerical restrictions in text boxes
☐ Other:

XI. RETENTION

1) What are the retention periods for the information?

Retention periods are currently being reviewed to establish and implement appropriate retention schedule for all information in the system.

XII. SECURITY

1) What types of administrative safeguards protect the information?
☒ Contingency Plan
☐ User manuals for the system
☒ Rules of Behavior
☒ Non-Disclosure or other contractual agreement
☐ Other:

2) What types of physical safeguards protect the information?
☐ Guards
☐ Identification Badges
☐ Biometric
☐ Cameras
☐ Physically secured space with need to know access
☒ Other: *All physical safeguards that are present at the AWS computing centers*

3) What types of technical safeguards protect the information?
   ☒ User Identification
   ☒ Firewall
   ☒ Virtual Private Network (VPN)
   ☒ Multi-factor Authentication (MFA)
   ☒ Passwords
   ☒ Encryption
   ☐ De-Identification
   ☐ Anonymization
   ☐ Other:

4) What monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate use of the information?

   The environment has in place alerts, audit logging, and reporting capabilities to ensure that the system operators receive information regarding unauthorized access to the environment, and potential inappropriate use of the information. These safeguards use a collection of the AWS Simple Notification Service (SNS), Cloudwatch logging, and Cloud Health.

5) Is this system hosted by a Cloud Service Provider (CSP)? Yes.
   a. If yes, which one? Amazon Web Services Commercial Cloud
   b. If yes, has the system obtained a FedRAMP Authorization? Yes.

XIII. TRAINING

1) What privacy training is provided to users of the system?

   All CFTC staff are required to take annual security and privacy training. No system-specific privacy training is given at this time.