Privacy Impact Assessment
for
Order Book On-Demand-Market Financial Data Cloud (OBOD-MFDC)

January 2025

System/Business Owner

Kenneth O'Brien
Associate Director, Data Engineering and Architecture Section
Division of Data

Reviewing Official

Kellie Cosgrove Riley
Chief Privacy Officer

I. SYSTEM OVERVIEW

1) Describe the purpose of the system/collection:

Order Book On-Demand-Market Financial Data Cloud (OBOD-MFDC) is an evolution of the Order Book on Demand (OBOD) cloud environment that originally allowed for the storage, loading, and analysis of Order Book data. The expansion of the OBOD environment to OBOD-MFDC allows for the storage, hosting, and analysis of all market and financial data sets used by the Commodity Futures Trading Commission (CFTC) in the former OBOD-only authority to operate (ATO) boundary in an Amazon Web Services (AWS) cloud environment.

The OBOD-MFDC is comprised of:

- Trade Capture Report (TCR)
- Regulatory Statement Review (RSR)
- Commission and Staff Letter (CSLetters)
- Fillings and Actions (FILAC)
- Integrated Surveillance System (ISS)
- Legal Entity Identifier (LEI)
- National Futures Association (NFA)
- Part 16 Volume, Price and Date Data Reports (PT16SEF)
- Part 20 Interim Report
- Part 20 Swaps LTR
- Part 20 Physical Commodity Swaps Data
- Part 39 DCO Cleared Swaps
- Part 39 Margin and Collateral Data
- Part 45 Harmonized SDR 2.0
- Pool Quarterly Report (PQR)
- Product Reference File (PRF)
- CAR file
- Customer Gross Margin Report
- IRS Margin & Position Data
- Order Book
- Swaps Reference Data

These data sets are collected by CME other external entities and provided to the CFTC in accordance with the Commodity Exchange Act (CEA). They are routinely stored and accessed in the CFTC's Market Financial System (MFS)IData Engineering & Processing (DEAP) (MFS-DEAP)

boundary and provided to OBOD-MFDC. This includes data from CFTC Form 40 and Form 102 (statements from the Ownership and Control Report (OCR) data streams) provided to OBOD-MFDC by MFS-DEAP.

Data sets can only be added to the environment on the approval of a Change Request (CR) by the CFTC Change Control Board (CCB).

The mission facing divisions of the CFTC 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.

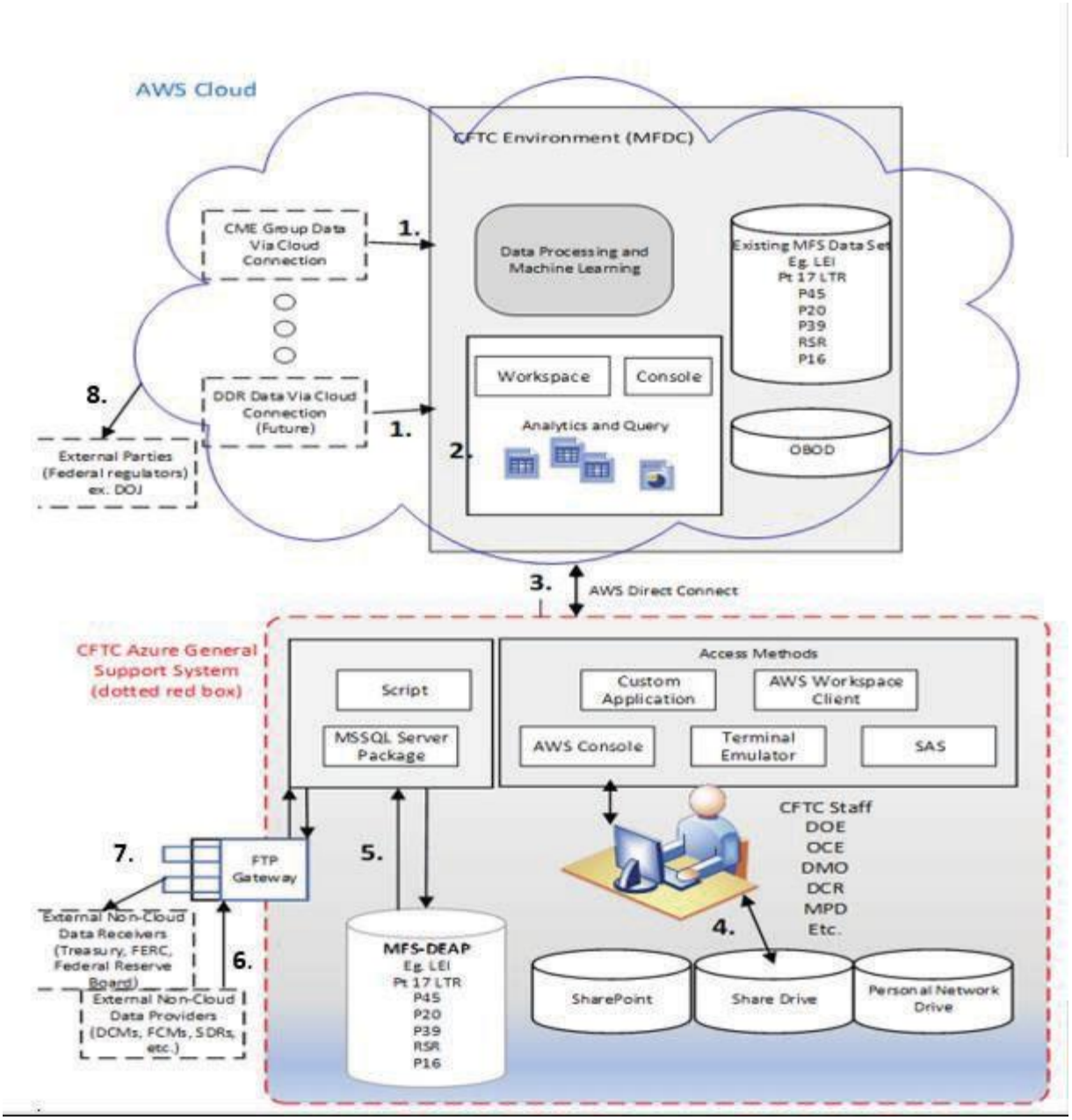

Figure 1. above shows the personally identifiable information (PII) data flow of the OBOD-MFDC environment.

1. Within the AWS cloud, certain reporting entities, such as the CME and the Depository Trust and Clearing Corporation Data Repository (DDR), are able to write in data buckets that are owned by the reporting entity, but readable by the CFTC.

2. OBOD-MFDC users consist of the DOE, DMO, and the DCR (AKA CFTC staff). Using

a native AWS workspace client, AWS console tool (such as Sagemaker), or on premises application that is leveraging the CFTC's AWS cloud environment, CFTC staff can access a variety of tools to perform research as well as market analysis and compliance activities on all data sets in the cloud. Advanced techniques such as machine learning that can be used to perform trend analysis or modeling.

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), or 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, or a connection to the AWS console.

4. If necessary, data can be exported from OBOD-MFDC by CFTC staff and stored in secure storage on the CFTC's on-premise (Microsoft Azure cloud) environment.

5. OBOD-MFDC receives PII from the CFTC Market Financial System (MFS)I Data Engineering & Processing (DEAP) (MFS-DEAP) which includes data from Form 40 and Form 102 (statements from the Ownership and Control Reporting (OCR) data streams.

6. Data is also provided by various external non-cloud providers including Designated Contract Markets (DCMs), Futures Commission Merchants (FCMs), Swap Dealers, Swaps Data Repositories (SDRs), Clearing Firms, and other participants in the Futures, Options, and Swaps markets. The data is provided to the CFTC through automated daily feeds and loaded into M FS-DEAP databases depending on the structure of the data where it will then be uploaded to OBOD-MFDC.

7. Data is provided to various external non-cloud data receivers to include the Department of the Treasury, the Federal Reserve Board, and the Federal Energy Regulatory Commission (FERC). These external non-cloud data receivers receive information regarding the futures and options markets. This data is extracted from OBOD-MFDC and provided to MFS-DEAP where it will then be shared with the external non-cloud data receiver.

8. Data from OBOD-MFDC 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.

II. AUTHORITY AND PURPOSE

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

The CFTC requires the information the system collects to perform basic market oversight functions including risk management, surveillance, and market liquidity analysis. The CFTC has authority to collect this information under the Commodity Exchange Act (CEA), 7 U.S.C. 1 et seq., and the Commission's regulations promulgated thereunder.

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	□ Sex
□ 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?

Within the AWS cloud, certain reporting entities, such as the CME and the DDR, are able to write in data buckets within OBOD-MFDC that are owned by the reporting entity, but readable by the CFTC. Data is also provided by various external data providers including Designated Contract Markets (DCMs), Futures Commission Merchants (FCMs), Swap Dealers, Swaps Data Repositories (SDRs), Clearing Firms, and other participants in the Futures, Options, and Swaps markets. The data provided by various external data providers is provided to the CFTC through automated daily feeds and loaded into MFS-DEAP databases depending on the structure of the data then uploaded to OBOD-MFDC.

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 investigations, position limit analysis, or risk analysis, the information within the OBOD-MFDC system is retrieved using a trader's name.

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?
   Staff in DOE, DMO, MPD, DOD, DA-IT and DCR may have access to the information to perform their job functions. The information may be shared internally among these offices or divisions where collaboration is required to perform their responsibilities.

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 some 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 a Memorandum of Understanding (MOU), Access Grant, or Non-Disclosure Agreement (NDA). 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-MFDC environment. 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 reporting parties as a result of a market participant's activity in the market. This PIA, CFTC-10, Investigatory Records (76 FR 5973) and CFTC-15, Enterprise Surveillance, Oversight & Risk Monitoring System (77 FR 58814) provide notice of the CFTC's collection of this information.

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?

The data in this environment is collected from the CFTC system MFS-DEAP, and from certain large reporting entities that are equipped to make cloud-to-cloud transfers of data. The latter is outside of the OBOD-MFDC boundary.

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?

The data collected is limited to that which is directly described in the CEA rules. The data represents information that is the minimum required for the analysis being performed by CFTC's divisions. 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?

The OBOD-MFDC data is subject to the following CFTC Mission Schedules:
602 - Market, Financial, and Other Data Submissions; destroys between 20 years and 40 years after submission
603 - Noteworthy Market Events; destroys 50 years after identified event
604 - Summary of Data Submissions; destroys 75 years after submission

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), GuardDuty, CloudWatch logging, and Cloud Health. Additionally, the CFTC has developed dashboards using the AWS QuickSight product which allows staff to assess the state of data loading activities throughout the environment.

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 awareness training. New users are required to attend a training session that describes their security responsibilities in the AWS environment.