KOR

KOR SEC SBSDR Disclosure Document | Version 1.2

Policy

KOR Public

KOR Public

Effective: August 9, 2023

Approved By: Tara Manuel

Table of Contents

0 Overview

This Disclosure Document is provided to you pursuant to SEC Regulation 13n-10(b).

Terms used but not defined in this Disclosure Document shall have the meaning ascribed to such terms in the KOR SEC Rulebook, which is publicly available on the KOR website: https://www.korfinancial.com

1.0 Criteria for providing access to KOR SBSDR

Market Participant's requirements to access the SBSDR are outlined in the KOR SBSDR Rulebook section "Client Access to Data" which is also provided below.

1.1 Procedures for gaining access to KOR SBSDR

KOR SBSDR provides services as a Securities-Based Swap Data Repository ("SBSDR" or "SDR"). These services are available to all Market Participants on a fair, open, and equal basis. In order to obtain access to the KOR SBSDR, a Market Participant must execute the KOR Universal Services Agreement and applicable Addendums. The KOR SBSDR does not, and will not, tie or bundle the offering of mandated regulatory services with ancillary services offered by KOR SBSDR or a KOR Affiliate.
Details on how to become a Client of KOR SBSDR can be found in the Client Onboarding Guide.

KOR SBSDR imposes the following qualifications on Clients of the KOR SBSDR (collectively, the "Client Criteria"):

a. A valid LEI;

b. Execution of the KOR Universal Services Agreement ("KOR USA") and applicable Addendums;

c. Compliance with the KOR SBSDR Rulebook and KOR Technical Specifications as published by KOR SBSDR (The KOR SBSDR Technical Specifications include all CFTC Technical Specifications in addition to KOR SBSDR's additional fields and validations.); and

d. Successful passing of KOR Know Your Customer (KYC) procedures, which will include but limited to compliance with Applicable Law, specifically those related to sanctions administered and enforced the by the Office of Foreign Assets Control of the U.S. Department of the Treasury ("OFAC").

As a general policy, KOR SBSDR requires all applicants to execute and submit KOR Universal Services Agreement and applicable addendums in electronic form only. Paper copies will not be accepted.

In the event a Client at any point fails to comply with any or all of the Client Criteria, such Client shall notify KOR immediately upon discovery. Notice must include a description of all relevant events associated with the failure, planned remediation where applicable, and any other information reasonably requested by KOR.

1.2 Client Rules & Applicable Law

By entering into the KOR USA, each Client agrees to be bound by the terms of the USA, the KOR SEC Rulebook, and any published policies and guides.

KOR and its Clients are subject to all Applicable Law including Applicable Regulations relevant to the Client or the transaction associated with such Client. Any Applicable Law affecting the (i) duties or obligations of KOR SBSDR or (ii) the performance of any Client shall take precedence over the rules of the KOR SBSDR Service. In the event of a conflict between Applicable Law and the rules of the KOR SBSDR Service, Applicable Law shall prevail.

1.3 Delegated Reporter Client access

Where a Client has authorized a Third-party Reporter or Related Entity Client under the same Parent to submit on its behalf and access its data, KOR will provide access to the Third-party Reporter or Client as long as it has executed the appropriate KOR Universal Services Agreement and applicable addendums and the Client has granted permission through the Client Portal. Related Entity Clients and Third-party Reporters are together referred to as Delegated Reporters.

1.4 Authorized Access Client access

Where a Client has authorized a Third-party Client to access its data, but not submit on its behalf, KOR will provide access to the Authorized Access Client as long as it has executed the appropriate KOR Universal Services Agreement and applicable addendums and the Client has granted permission through the Client Portal.

1.5 Users

1.5.1 Administrative Users

Clients are required to maintain at least two Administrative Users on KOR’s SBSDR System. This information must be provided when executing the KOR Universal Services Agreement and applicable addendums. The correct contact information must be kept up to date at all times.

Administrative Users are responsible for creating, managing, and removing access to their company’s Users and to other Clients who are eligible to access the KOR SBSDR System on

behalf of the Client including Third-party Client access. Administrative Users will be the main point of contact for KOR's Client Services in regard to urgent issues.

1.5.2 Access to trades, related data, and reports

Any Market Participant that has executed a Client Agreement may access SBSBSDR Data to which they are a party to or for which they have been granted access to on behalf of a Client. Access to KOR SBSDR is strictly limited to active Users with valid permissions created by their Client's Administrative User.

Upon set up, Users will be provided logins and the ability to access data in the KOR SBSDR. Access is driven off the Client's LEIs for which the User has been associated. Users may be granted access to multiple LEIs under the same Parent as related entities.

The KOR SBSDR System will allow Users to view full trade details associated with any individual swap and all associated messages, errors and reports which they have permission to view where their Client LEI is one of the following fields (Fields are defined in the KOR Technical Specifications):

a. Central counterparty
b. Clearing member
c. Counterparty 1
d. Counterparty 2
e. Submitter identifier
f. Reporter identifier (his field was added by KOR to identify who the Submitter identifier is submitting on behalf of for access validation. This will not always be counterparty 1, as the Submitter may be a Delegated Reporter for a Platform with the requirement to report.)
g. Counterparty 1 Agent (KOR SBSDR has added the Agent field in order to correctly permission investment managers to view trades where they were the execution agent but are not the counterparty or submitter.)
h. Counterparty 2 Agent (OR SBSDR has added the Agent field in order to correctly permission investment managers to view trades where they were the execution agent but are not the counterparty or submitter.

For swaps executed On Facility, the Platform may access the swap that they had the requirement to report, but not any data subsequently reported by the Reporting Side.

Clearing Members that have executed the appropriate KOR Universal Services Agreement and applicable Addendums may access swaps where they are listed as the Clearing Member.

Investment Managers that have executed the appropriate KOR Universal Services Agreement and applicable Addendums and been granted access from their managed funds which are Clients, may access swaps where they are a counterparty or the executing agent.

1.5.3 Anonymous execution

SBSDR Data and SBSDR Information related to a particular swap transaction that is maintained by KOR SBSDR may be accessed by either counterparty to that particular swap. However, the SBSDR Data and SBSDR Information maintained by KOR SBSDR that may be accessed by either counterparty to a particular swap shall not include the identity or the legal entity identifier of the other counterparty to the swap, or the other counterparty's clearing member for the swap, if the swap is executed anonymously on a Platform and cleared at a derivatives clearing authority ("CA"). This also applies to any Client accessing data on another Client's behalf acting as that party, including Delegated Reporters, Authorized Access Clients, and investment managers.

1.5.4 Review of Market Participant access to KOR SBSDR

Client's designated Administrative Users are expected to maintain correct User access at all times. In addition, following the end of each calendar quarter, all Clients will have access to a report on current User's access levels and a list of all Client's they have granted access to their data. At least one of the designated Administrative Users at each Client must review the listing of Users and other party access and confirm whether access should be maintained, removed or changed and make the appropriate updates.

When one or both of the Client's designated Administrative Users needs to be amended, the Client must contact KOR Client Service (support@korfinancial.com).

Records of all User access are maintained and available for review by the Client and KOR Compliance at all times.

2.0 Criteria for Market Participants seeking to connect to the SBSDR

In order to submit data to KOR SBSDR, a Market Participant must first become a Client by executing the KOR Universal Services Agreement and applicable SBSDR Addendums and then write to the KOR SBSDR API. KOR uses JSON format for its API. The fields and validations for submission are defined in the KOR Technical Specifications, details for writing to the KOR SBSDR API will be provided to Client's in the KOR SBSDR API documentation. Market Participants that only require view access must execute a Client Agreement and then can query and view their data via a web-based UI without writing to the KOR API.

3.0 Policies and procedures regarding the SBSDR's safeguarding of SBSDR Data and operational reliability to protect the confidentiality and security or SBSDR Data

KOR has implemented corporate policies to ensure that confidential information is treated appropriately and managed in alignment with business goals and in accordance with legal and regulatory requirements and professional standards.

Please reference the KOR SBSDR Rulebook section "System Safeguards" which is also provided below.

3.1 Systems testing

KOR SBSDR shall conduct regular, periodic, objective testing and review of its automated systems to ensure that they are reliable, secure, and have adequate scalable capacity. It shall also conduct regular, periodic testing and review of its business continuity-disaster recovery capabilities.

3.2 Systems testing planning

To the extent practicable, KOR shall:

a. Where possible, coordinate with Clients and service providers to participate in synchronized testing in a manner adequate to enable effective resumption of KOR SBSDR's fulfillment of its duties and obligations following a disruption causing activation of KOR SBSDR's business continuity and disaster recovery plan;

b. Participate in periodic, synchronized testing of its business continuity and disaster recovery plan and the business continuity and disaster recovery plans of its Clients, and the business continuity and disaster recovery plans required, as applicable, by each appropriate prudential regulator, the Financial Stability Oversight Council, the Securities and Exchange Commission, the Department of Justice or any other person deemed appropriate by the SEC; and

c. Ensure that its business continuity and disaster recovery plan take into account the business continuity and disaster recovery plans of its telecommunications, power, water, and other essential service providers.

4.0 Policies and procedures to protect the privacy of SBSDR Data

KOR SBSDR has implemented policies and procedures to protect the privacy of SBSDR Data. In order to gain access to non-public data a Market Participant must first become a Client of the SBSDR as described in the KOR SDR Rulebook section: "Client access to data."

Please reference the KOR Privacy Policy which is publicly available on the KOR website (https://www.korfinancial.com/privacy-policy).

5.0 Policies and procedures regarding the SBSDR's non-commercial and/or commercial use of SBSDR Data

Generally, data accepted and maintained by the SBSDR may not be used for commercial or business purposes by the security-based swap data repository or any of its affiliated entities.

KOR SBSDR has implemented adequate "firewalls" or controls to protect the reported SBSDR data required to be maintained under SEC regulations from any improper commercial use.

However, a Client that submits SBSDR data maintained by the SBSDR, may permit the commercial use by providing express written consent. Such consent shall not be a requirement to report to the SBSDR. If such Client consent is given, KOR may not make such consented data available for commercial use prior to its public dissemination.

6.0 Dispute resolution procedures

The dispute resolution procedures are outlined in the KOR SBSDR Rulebook section "Dispute Resolution" which is also provided below.

KOR has established procedures and provides facilities for effectively resolving disputes over the accuracy of the SBSDR Transaction Data and positions that are recorded in the SBSDR.

When the Reporting Side does not agree with the accuracy of the reporting of a security-based swap or a position in KOR SBSDR, but is prevented from amending the swap to what they believe to be accurate, the Client must follow the following steps:

a. Enter a ticket with KOR SBSDR support with the details of the issue; and
b. Submit an allowed value per the KOR Technical Specifications for the KOR SBSDR field that reflects the dispute. The allowed values are a high-level indication of the issue. Sample values may include but are not limited to: "No accurate UPI available" or "KOR Technical Specifications do not allow for accurate representation". Clients may contact KOR SBSDR to add additional values, but these values will be at the discretion of KOR SBSDR.

7.0 Description of KOR SBSDR services

KOR SBSDR is registered for and accepts data in the following Asset Classes: credit default, interest rates, and equities. To maintain its SBSDR status, KOR shall continue to demonstrate

substantial compliance with all applicable provisions of its orders and applicable rules and regulations under applicable SEC Rules.

Details regarding the SBSDR are outlined in the KOR SBSDR Rulebook, in sections: “Client duties and obligations regarding SEC Rule 242.900-909 data,” “Client data reporting standards,” “Unique Identifiers”, “SBSDR duties and obligations regarding securities-based swaps reporting,” “Publicly disseminated security-based swaps,” and “ SBSDR System” which are also provided below.

7.1 Client duties and obligations regarding SEC Rule 242.900-909 data

7.1.1 Assigning reporting duties

A security-based swap, including a security-based swap that results from the allocation, termination, novation, or assignment of another security-based swap, shall be reported as follows.

7.1.1.1 Platform-executed security-based swaps that will be submitted to clearing

If a security-based swap is executed on a platform and will be submitted to clearing, the platform on which the transaction was executed shall report to a registered security-based swap data repository the counterparty ID or the execution agent ID of each direct counterparty, as applicable, and the information set forth in SEC Rule 242.901(c) (except that, with respect to SEC Rule 242.901 (c)(5)), the platform need indicate only if both direct counterparties are registered security-based swap dealers) and SEC Rule 242.901 (d)(9) and (10).

7.1.1.2 All other security-based swaps

For all security-based swaps other than platform-executed security-based swaps that will be submitted to clearing, the reporting side shall provide the information required by SEC Rule(s) §§ 242.900 through 242.909 to a registered security-based swap data repository. The reporting side shall be determined as follows.

7.1.1.3 Clearing transactions

For a clearing transaction, the reporting side is the registered clearing agency that is a counterparty to the transaction.

7.1.1.4 Security-based swaps other than clearing transactions

The reporting side shall be determined as follows:

a. If both sides of the security-based swap include a registered security-based swap dealer, the sides shall select the reporting side.

b. If only one side of the security-based swap includes a registered security-based swap dealer, that side shall be the reporting side.

c. If both sides of the security-based swap include a registered major security-based swap participant, the sides shall select the reporting side.

d. If one side of the security-based swap includes a registered major security-based swap participant and the other side includes neither a registered security-based swap dealer nor a registered major security-based swap participant, the side including the registered major security-based swap participant shall be the reporting side.

e. If neither side of the security-based swap includes a registered security-based swap dealer or registered major security-based swap participant:

    i. If both sides include a U.S. person, the sides shall select the reporting side.

    ii. If one side includes a non-U.S. person that falls within SEC Rule(s) § 242.908(b)(5) or a U.S. person and the other side includes a non-U.S. person that falls within SEC Rule(s) § 242.908(b)(5), the sides shall select the reporting side.

    iii. If one side includes only non-U.S. persons that do not fall within SEC Rule(s) § 242.908(b)(5) and the other side includes a non-U.S. person that falls within SEC Rule(s) § 242.908(b)(5) or a U.S. person, the side including a non-U.S. person that falls within SEC Rule(s) § 242.908(b)(5) or a U.S. person shall be the reporting side.

    iv. If neither side includes a U.S. person and neither side includes a non-U.S. person that falls within SEC Rule(s) § 242.908(b)(5) but the security-based swap is effected by or through a registered broker-dealer (including a registered security-based swap execution facility), the registered broker-dealer (including a registered security-based swap execution facility) shall report the counterparty ID or the execution agent ID of each direct counterparty, as applicable, and the information set forth in SEC Rule(s) § 242.901(c) (except that, with respect to SEC Rule(s) § 242.901(c)(5), the registered broker-dealer (including a registered security-based swap execution facility) need indicate only if both direct counterparties are registered security-based swap dealers) and SEC Rule(s) § 242.901(d)(9) and (10).

7.2 Client data reporting standards

7.2.1 Data reported to Securities-Based Swap Data Repositories

In reporting required security-based swap data and required life-cycle event data to KOR SBSDR, each Reporting Side shall report the Security-Based Swap Data elements in the form and manner provided in the technical specifications published by KOR SBSDR in the form and manner provided in the KOR Technical Specifications.

In reporting required security-based swap data to KOR SBSDR, each Client making such report shall satisfy the Security-Based Swap Data Validation Procedures of KOR SBSDR.

In reporting Security-Based Swap Data to KOR SBSDR, each Client shall use the facilities, methods, or data standards provided and required by KOR SBSDR.

The fields, validations, and methods are published in the KOR Technical Specifications.

7.2.2 Data Validation

KOR SBSDR shall validate SBSDR Data ASATP after such data is accepted according to the validation conditions set forth in the KOR Technical Specifications including any validations KOR SBSDR deems necessary to meet the SBSDR Regulations.
For each required security-based swap data report submitted to KOR SBSDR, the Security-Based Swap Data Repository shall notify the Submitter of the report whether the report satisfied the Security-Based Swap Data validation procedures. KOR SBSDR shall provide such notification ASATP after accepting the report.

If the submitted SBSDR Data contains one or more data validation errors, KOR SBSDR shall distribute a Data Validation Error Message to the Client that submitted such SBSDR Data ASATP after acceptance of such data. Each Data Validation Error Message shall indicate which specific data validation error(s) were identified in the SBSDR Data. Where technologically practicable, the KOR SBSDR will process all validations for the submission and return all applicable validations errors to the Client.

If a required security-based swap report to KOR SBSDR does not satisfy the Data Validation Procedures of the Security-Based Swap Data Repository, the Reporting Side required to submit the report has not yet satisfied its obligation to report required security-based swap data within the timelines set forth in SEC Rule(s). The Reporting Side has not satisfied its obligation until it submits the required Security-Based Swap Data report per the KOR SBSDR Technical Specifications which includes the requirement to satisfy the Data Validation Procedures of the KOR SBSDR.

Public messages and must be submitted independently but provide the required information to tie the two to the same UTI.

7.3 Unique Identifiers

7.3.1 Coded information

KOR will not provide reports on missing UICs to its Clients per the SEC Cross-Border Release no action: With respect to Rule 906(a) of Regulation SBSR, if a registered SDR does not send reports of missing unique identification codes to its participants.

7.3.1.1 Unique Trade Identifiers (UTI)

Each swap shall be identified in all recordkeeping and all Security-Based Swap Data reporting by the use of a unique trade identifier, which shall be created, transmitted, and used for each swap.

Each registered entity and swap counterparty shall include the unique trade identifier for a swap in all of its records and all of its Security-Based Swap Data reporting concerning that swap, from the time it creates or receives the unique trade identifier as provided in this section, throughout the existence of the security-based swap and for as long as any records are required by the Act or Commission regulations to be kept concerning the security-based swap, regardless of any life-cycle events concerning the security-based swap, including, without limitation, any changes with respect to the counterparties to the security-based swap.

KOR SBSDR shall not allow any trade executed on or after UTIs are implemented to be submitted with a Unique Swap Identifier (“USI”) in lieu of a UTI.

Every submission to KOR SBSDR shall contain the appropriate UTI, otherwise the submission will be rejected. KOR SBSDR shall validate the format and uniqueness of every UTI. If a party submits the incorrect UTI, they must error that UTI and resubmit the swap as a new message with the correct UTI. When the correct UTI is submitted it will be considered a new trade and if it is submitted after the required reporting timelines, will be classified as a late report.

7.3.1.2 Use of the legal entity identifier

Each party to a swap shall use legal entity identifiers to identify itself and swap counterparties in all recordkeeping and all Security-Based Swap Data reporting. If a security-based swap counterparty is not eligible to receive a legal entity identifier as determined by the Global Legal Entity Identifier System, such counterparty shall be identified in all recordkeeping and all Security-Based Swap Data reporting with an Natural Person identifier. It is the duty of the Reporting Side to always submit a unique and consistent Natural Person Identifier. In order to consistently submit a unique value, the LEI of the Reporting Side followed by natural person’s email shall be used for the identifier.

Each Client shall maintain and renew its legal identity identifier in accordance with the standards set by the Global Legal Entity Identifier System.

Per the KOR SBSDR Technical Specification, KOR SBSDR shall not accept messages that do not contain LEIs published by GLEIF. The exception being fields which allow Natural Person Identifiers, no other identifier types will be accepted. KOR SBSDR shall not accept LEIs with a status of “INACTIVE” on GLEIF. If an LEI is published under a Local Operating Unit, but is not on GLEIF, it will not be accepted.

Neither the counterparty 1 nor counterparty 2 LEI may be updated by a submission. In the event the incorrect LEI was submitted the UTI must be Errored, and a new security-based swap reported with a new UTI. In the event of a corporate action updates a UTI, the Reporting Side must notify KOR SBSDR. KOR SBSDR shall validate the change on GLEIF and update the LEI on all applicable records.

If a Reporting Side ports swaps in from another SBSDR that used a substitute identifier, those swaps shall be ported in using the correct LEI or if the party is not eligible for an LEI then the Natural Person Identifier.

7.3.1.3 Unique Product Identifiers (UPI)

Once UPIs are available, each swap shall be identified in all recordkeeping and all Security-Based Swap Data reporting by means of a unique product identifier and product classification system. Each swap sufficiently standardized to receive a unique product identifier shall be identified by a unique product identifier. Each swap not sufficiently standardized for this purpose shall be identified by its description using the product classification system.

Until UPIs are available, each registered entity and Security-Based Swap counterparty shall report product fields per the KOR SBSDR Technical Specifications.

7.4 KOR SBSDR duties and obligations regarding securities based swaps reporting

7.4.1 Time stamping incoming information

KOR SBSDR time stamps, to the second, its receipt of any information submitted to it pursuant to SEC Rule(s) § 242.901 (c), (d), (e), or (i).

7.4.2 Prevent invalidation or modification of data

KOR SBSDR has established systems and User access restrictions reasonably designed to prevent any provision in a valid swap from being invalidated or modified through its verification or recording process. Client Agreements contain language intended to prevent any such invalidation or modification.

7.4.3 Error corrections

KOR shall:

a. Upon discovery of an error or receipt of a notice of an error, verify the accuracy of the terms of the security-based swap and, following such verification, promptly correct the erroneous information regarding such security-based swap contained in its system; and

b. If such erroneous information relates to a security-based swap that the registered security-based swap data repository previously disseminated and falls into any of the categories of information enumerated in SEC Rule § 242.901(c), publicly disseminate a corrected transaction report of the security-based swap promptly following verification of the trade by the counterparties to the security-based swap, with an indication that the report relates to a previously disseminated transaction.

KOR has implemented systemic measures to help ensure that all Client submissions are accurately reflected in the KOR SBSDR. The onus lies on the Client to flag all submissions with the applicable Action and Event type. Amended records are saved as a new version while keeping the older version(s) for tracking changes that occurred on the trade. KOR employs active monitoring and alerting of system component general health and specific processes to ensure the continuous operation of data processing. Specifically: (i) All message processing errors and exceptions at the message level are logged and monitored 24/7 by the monitoring system.; and (ii) Monitoring and alerting if the database/application server and other processes are down or unreachable.

The KOR SBSDR shall accept error corrections for SBSDR Data. Error corrections include corrections to errors and omissions in SBSDR Data previously reported to the Security-Based Swap Data Repository, as well as omissions in reporting SBSDR Data for security-based swaps that were not previously reported to a Security-Based Swap Data Repository. The requirement to accept error corrections applies for all swaps, regardless of the state of the security-based swap that is the subject of the SBSDR Data. This includes security-based swaps that have terminated, matured, or are otherwise no longer considered to be open security-based swaps, provided that the record retention period has not expired as of the time the error correction is reported. KOR SBSDR shall record the corrections, as soon as technologically practicable after the KOR SBSDR accepts the error correction.

All error corrections are recorded in accordance with KOR’s recordkeeping policies and procedures. KOR SBSDR disseminates corrected data to the public and the SEC, as applicable, in

accordance with its dissemination policies and procedures.

7.4.4 Recordkeeping for Transaction Data

KOR SBSDR shall maintain transaction data and related identifying information for not less than five years after the applicable security-based swap expires and historical positions for not less than five years:

a. In a place and format that is readily accessible and usable to the Commission and other persons with authority to access or view such information; and

b. In an electronic format that is non-rewriteable and non-erasable.

7.4.5 Positions

KOR SBSDR shall calculate Position views of data. These views will include the gross and net notional amount, by leg, for all open security-based swaps. For security-based swaps executed in a notional other than USD, the notional in USD must be submitted for KOR to aggregate open security-based swaps in a single currency, USD.

7.5 Publicly disseminated security-based swaps

7.5.1 Real-time public reporting

Except as provided in SEC Rule(s) § 242.901(c), a registered security-based swap data repository shall publicly disseminate a transaction report of a security-based swap, or a life cycle event or adjustment due to a life cycle event, immediately upon receipt of information about the security-based swap, or upon re-opening following a period when the registered security-based swap data repository was closed. The transaction report shall consist of all the information reported pursuant to SEC Rule(s) § 242.901(c), the Primary Trade Information, plus any condition flags contemplated by the registered security-based swap data repository's policies and procedures that are required by § 242.907. The fields required to be reported and how they are disseminated are defined in the KOR Technical Specifications.

KOR SBSDR will establish electronic systems as necessary to accept and disseminate data in connection with real-time public reporting pursuant to SEC rules for all security-based swaps in its approved Asset Classes. KOR SBSDR will publicly report Security-Based Swap Transaction and Pricing Data on each publicly reportable swap where a public dissemination message is received.

KOR SBSDR shall Publicly Disseminate Security-Based Swap Transaction and Pricing Data ASATP after such data is received. If the Client wishes for the trade to not be disseminated until the end

of the 24 business hour reporting window, it is the duty of the submitting Client to hold the submission until the time they wish for it to be disseminated.
For all transactions which require public dissemination under SEC rules, Clients submitting data are required to report all fields in accordance with the KOR Technical Specification.
References: SEC Rule(s) §242.902(a).

Note:
KOR shall apply the SEC Cross-Border Release no action: With respect to Rule 902 of Regulation SBSR, if a registered SDR does not disseminate an SBS transaction in a manner consistent with Rule 902 but instead disseminates (or does not disseminate) the SBS transaction in a manner consistent with Part 43 of the CFTC's swap reporting rules in force at the time of the transaction, provided that for an SBS based on a single credit instrument or a narrow-based index of credit instruments having a notional size of $5 million or greater, the registered SDR that receives the report of the SBS transaction does not utilize any capping or bucketing convention under Part 43 of the CFTC's swap reporting rules but instead disseminates a capped size of $5 million (e.g., “$5MM+” or similar) in lieu of the true notional size.[768]

SEC Cross-Border Release no action: With respect to Rule 907(a)(4) of Regulation SBSR, if a registered SDR does not have policies and procedures for establishing and directing its participants to use condition flags in the reporting of SBS transactions, provided that the registered SDR instead complies with analogous CFTC rules regarding condition flags or other trade indicators.

7.5.2 Availability of Security-Based Swap Transaction and Pricing Data to the public

KOR SBSDR shall make Security-Based Swap Transaction and Pricing Data available on the KOR website for one year after the initial Public Dissemination of such data and shall make instructions freely available on said website on how to download and search such data. Security-Based Swap Transaction and Pricing Data that is Publicly Disseminated shall be made available free of charge.

7.5.3 Security-Based Swap Transaction and Pricing Data to be Publicly Disseminated in real-time

KOR SBSDR shall Publicly Disseminate the information described in SEC rules for the Security-Based Swap Transaction and Pricing Data, as applicable, in the form and manner provided in the KOR Technical Specifications.

KOR SBSDR shall require any data and fields necessary to compare the Security-Based Swap Transaction and Pricing Data that was Publicly Disseminated in real-time to the data reported to a

Security-Based Swap Data Repository. Such additional information shall not be Publicly Disseminated by KOR SBSDR.

7.5.4 Non-disseminated information

KOR will not disseminate:

a. The identity of any counterparty to a security-based swap;

b. With respect to a security-based swap that is not cleared at a registered clearing agency and that is reported to the registered security-based swap data repository, any information disclosing the business transactions and market positions of any person;

c. Any information regarding a security-based swap reported pursuant to § 242.901(i);

d. Any non-mandatory report;

e. Any information regarding a security-based swap that is required to be reported pursuant to SEC Rule(s) §§ 242.901 and 242.908(a)(1) but is not required to be publicly disseminated pursuant to § 242.908(a)(2);

f. Any information regarding a clearing transaction that arises from the acceptance of a security-based swap for clearing by a registered clearing agency or that results from netting other clearing transactions;

g. Any information regarding the allocation of a security-based swap; or

h. Any information regarding a security-based swap that has been rejected from clearing or rejected by a prime broker if the original transaction report has not yet been publicly disseminated.

It is the duty of the Reporting side to not submit public dissemination messages to KOR that do not apply for public dissemination.

7.5.5 Temporary restriction on other market data sources

No person shall make available to one or more persons (other than a counterparty or a post-trade processor) transaction information relating to a security-based swap before the primary trade information about the security-based swap is sent to a registered security-based swap data repository.

7.5.6 Anonymity of the parties to a Publicly Reportable Security-Based Swap Transaction

Security-Based Swap Transaction and Pricing Data that is Publicly Disseminated in real-time shall not disclose the identities of the parties to the security-based swap or otherwise facilitate the

identification of a party to a security-based swap. KOR SBSDR shall not Publicly Disseminate such data in a manner that discloses or otherwise facilitates the identification of a party to a security-based swap.

KOR SBSDR requires Clients to provide the KOR SBSDR with Security-Based Swap Transaction and Pricing Data that includes an actual description of the underlying asset(s). KOR SBSDR Publicly Disseminates the actual underlying asset(s) of all Publicly Reportable Swap Transactions.

8.0 KOR SBSDR Fee Schedule

Fees are assessed in a consistent, non-preferential manner and are not permitted to be used as a barrier to entry. KOR SBSDR will not offer preferential pricing arrangements to any Client on any basis, including volume discounts or reductions unless such discounts or reductions apply to all Clients uniformly and are not otherwise established in a manner that would effectively limit the application of such discount or reduction to a select number of Clients.

KOR shall ensure that any dues, fees, or other charges imposed by, and any discounts or rebates offered by, a security-based swap data repository are fair and reasonable and not unreasonably discriminatory. Such dues, fees, other charges, discounts, or rebates shall be applied consistently across all similarly-situated users of such security-based swap data repository's services, including, but not limited to, market participants, market infrastructures (including central counterparties), venues from which data can be submitted to the security-based swap data repository (including exchanges, security-based swap execution facilities, electronic trading venues, and matching and confirmation platforms), and third party service providers
All fees are fully disclosed and available on the KOR SBSDR website (www.korfinancial.com).

Changes to the KOR SBSDR fee schedule will be consistent with the principles set forth in this section.

9.0 SBSDR’s Governance Arrangements

The SBSDR’s governance arrangements are outlined in the KOR SBSDR Rulebook section “Corporate Structure,” and the Governance Principles document available on KOR’s website (https://www.korfinancial.com/key-documents).

9.1 Corporate structure

9.1.1 Board of Directors

The following Governance Principles have been adopted by the Board of Directors (the “Board”) of KOR Reporting Inc. (the “Company”) to serve as a flexible framework to assist the Board in the

exercise of its responsibilities. These Governance Principles reflect the Board's commitment to monitor the effectiveness of policy and decision making both at the Board and management level. These governance principles should be interpreted in the context of all applicable laws, KOR Reporting's Bylaws, other governing legal documents and company policies. These governance principles are subject to modification from time to time by the Board.

9.1.1.1 Mission Statement of the Board of Directors

The Board believes that all directors represent the balanced interests of the Company as a whole.

It represents the stakeholders' interest in perpetuating a successful business and optimizing long-term financial returns consistent with legal requirements and ethical standards. The Board also recognizes the important role the Company plays in the marketplace and the importance of providing active governance designed to ensure the safety and soundness of its operations. The Board is responsible for establishing the general oversight framework, including identifying and taking reasonable actions, intended to achieve these goals.

The Board's principal oversight functions are to:

a. Review, approve and monitor the Company's major strategic, financial and business activities and opportunities, including declarations of dividends and major transactions;
b. Review, approve and monitor the Company's annual budget;
c. Review, monitor and take reasonable actions with respect to the Company's financial performance;
d. Review, assess and provide oversight of the Company's risk management practices, the integrity and adequacy of its enterprise risk management program, which is designed to identify, manage and plan for its Security-based Swap Data Repository, compliance, financial, operational, reputational, and strategic and commercial risks;
e. Select, evaluate and compensate the Chief Compliance Officer and, if necessary, appoint a replacement;
f. Review and monitor plans for the succession of the Chief Executive Officer and other members of senior management.

9.1.2 Board membership and structure

9.1.2.1 Size of Board

The Board shall be comprised of at least three Directors. The size of the Board is designed to ensure it maintains the appropriate expertise, industry knowledge and skills to effectively oversee the Company's complex business while maintaining compliance with applicable listing and regulatory requirements.

9.1.2.2 Board Composition; Mix of Independent and Employee Directors

At least a majority of the directors will be independent directors as determined in accordance with the section "Determination of 'Independent' Directors" below (each an "*Independent Director*" and collectively the "*Independent Directors*"). The Board has adopted and disclosed categorical standards to assist it in determining a director's independence. The Board believes that it is often in the best interest of KOR Reporting to have non-Independent Directors. The expectation of the Board is that the number of directors who also serve as employees of the Company (each an "*Employee Director*" and collectively the "*Employee Directors*") should be at least one and fewer than the number of Independent Directors.

KOR provides representatives of market participants, including end-users, with the opportunity to participate in the process for nominating directors and with the right to petition for alternative candidates. The Board nomination process is covered under KOR's Governance Principles, Board nomination and selection.

9.1.2.3 Board Membership Criteria

The Board seeks directors from diverse professional backgrounds who combine a broad spectrum of experience and expertise with a reputation for integrity. Board members should have the characteristics essential for effectiveness as a member of the Board, including but not limited to:

a. Integrity, objectivity, sound judgment and leadership;
b. The relevant expertise and experience required to offer advice and guidance to the Chief Executive Officer and other members of senior management.
c. The ability to make independent analytical inquiries.
d. The ability to collaborate effectively and contribute productively to the Board's discussions and deliberations;
e. An understanding of the Company's business, strategy and challenges;
f. The willingness and ability to devote adequate time and effort to Board responsibilities and to serve of Committees at the request of the Board; and
g. Is not a Disqualified Person (as described below).

A "*Disqualified Person*" is any person who (i) is or has been subject to any statutory disqualification under Section 3(a)(39) of the Securities Exchange Act or Sections 8a (2)-(4) of the

Commodity Exchange Act or (ii) is or has been subject to disqualification under 17 CFR § 1.63.

Each Board member is expected to ensure that his or her other commitments do not materially interfere with his or her service overall as a director.

9.1.2.4 Determination of "Independent" Directors

The Board shall review annually the relationships that each director has with the Company (either directly or as a partner, equity holder or officer of an organization that has a relationship with the Company). Following such annual review, only those directors who the Board affirmatively determines have no material relationship with the Company (either directly or as a partner, equity holder, or officer of an organization that has a relationship with the Company) will be considered Independent Directors, subject to additional qualifications prescribed applicable law. Each director shall notify the Chairman and Chief Executive Officer as soon as practicable of any event, situation or condition that may affect the Board's evaluation of his or her independence.

9.1.2.5 Ethics and Conflicts of Interest

The Board has adopted a Conflict of Interest Policy. The Conflict of Interest Policy incorporates various provisions of applicable corporate law and other standards adopted by the Company to ensure that Board and committee decisions are not impacted by conflicts of interest. Directors are expected to avoid any action, position or interest that conflicts with an interest of the Company, or gives the appearance of a conflict, in accordance with the Conflict of Interest Policy and any rules adopted by the Company. The Company annually solicits information from directors in order to monitor potential conflicts of interest and directors are expected to be mindful of their fiduciary obligations to the Company.

When faced with a situation involving a potential conflict of interest, directors are encouraged to seek advice from the General Counsel or from outside counsel designated by the General Counsel.

Directors are expected to act in compliance with the Company's Board of Directors Code of Ethics.