KOR

KOR SEC SBSDR Rulebook | Version 1.2

Policy

KOR Public

KOR Public

Effective: January 22, 2024

Approved By: Tara Manuel

Table of Contents

0.1 Preamble 6

1.0 Defined terms 6

1.1 KOR Specific terms 6

2.0 No action relief 21

3.0 Corporate structure 21

3.1 Board of Directors 21

3.1.1 Mission Statement of the Board of Directors 22

3.2 Board membership and structure 22

3.2.1 Size of Board 22

3.2.2 Board Composition; Mix of Independent and Employee Directors 22

3.2.3 Board Membership Criteria 23

3.2.4 Determination of “Independent” Directors. 24

3.2.5 Ethics and Conflicts of Interest 24

4.0 Client access to data 24

4.1 Procedures for gaining access to KOR SBSDR 24

4.2 Client Rules & Applicable Law 25

4.3 Delegated Reporter Client access 25

4.4 Authorized Access Client access 26

4.5 Users 26

4.5.1 Administrative Users 26

4.5.2 Access to trades, related data, and reports 26

4.5.3 Anonymous execution 27

4.5.4 Review of Market Participant access to KOR SBSDR 28

5.0 Unique Identifiers 28

5.1 Coded information^6 28

5.1.1 Assigning UICs for entities^7 28

5.1.2 Assigning transaction ID 29

5.1.3 Public dissemination of coded information 29

5.2 Unique Trade Identifiers (UTI) 29

5.2.1 UTI Creation format 30

5.2.2 UTI Transmission 30

5.2.3 UTI Creation Entity 31

5.3 Legal Entity Identifiers (LEI) 31

5.3.1 Use of the legal entity identifier 31

5.4 Unique Product Identifiers (UPI) 32
5.4.1 KOR SBSDR’s temporary unique product identifier system 32
6.0 Client duties and obligations regarding SEC Rule 242.900-909 data 33
6.1 Assigning reporting duties 33
6.1.1 Platform-executed security-based swaps that will be submitted to clearing 33
6.1.2 All other security-based swaps 34
6.1.3 Clearing transactions 34
6.1.4 Security-based swaps other than clearing transactions 34
6.2 Notification to registered clearing agency 35
6.3 Interim timeframe for reporting 35
6.4 Trade information 36
6.5 Reporting of life cycle events 36
6.5.1 Acceptance for clearing 37
6.5.2 Life cycle reporting timeline 37
6.5.3 Interim timeframe for reporting 38
6.6 Format of reported information. 38
6.7 Reporting of pre-enactment and transitional security-based swaps 38
6.8 Other duties of participants 38
6.8.1 Policies and procedures to support reporting compliance 38
6.9 Cross-border matters 39
6.9.1 Application of Regulation SBSR to cross-border transactions 39
6.9.2 Limitation on obligations 40
6.9.3 Substituted Compliance 40
6.10 Life cycle event data reporting for security-based original swaps 40
6.11 Third-party facilitation of data reporting 41
6.12 Change of Security-Based Swap Data Repository 41
6.12.1 SBSDR Porting: Notifications 41
6.12.2 SBSDR Porting: Procedure 42
6.12.3 Changing Security-Based Swap Data Repository to KOR SBSDR 42
6.12.4 Changing Security-Based Swap Data Repository out of KOR SBSDR 43
7.0 Client data reporting standards 43
7.1 Data reported to Securities-Based Swap Data Repositories 43
7.2 Data Validation 44
8.0 Correction of errors in security-based swap information 45
8.1 Duty to correct 45

8.2 Form and manner for error correction 45
8.2.1 Non-Reporting parties 45
8.2.2 Exception 45
8.3 Verification that Security-Based Swap Data is complete and accurate 46
8.3.1 Method of verification 46
8.3.2 Delegated Reporters and Authorized Access Clients 47
9.0 KOR SBSDR duties and obligations regarding securities based swaps reporting 47
9.1 Time stamping incoming information 47
9.2 Prevent invalidation or modification of data 47
9.3 Error corrections 47
9.4 Recordkeeping for Transaction Data 48
9.5 Positions 49
10.0 Publicly disseminated security-based swaps^29 49
10.1 Real-time public reporting 49
10.2 Availability of Security-Based Swap Transaction and Pricing Data to the public 50
10.3 Security-Based Swap Transaction and Pricing Data to be Publicly Disseminated in real-tim 50
10.4 Non-disseminated information 51
10.5 Temporary restriction on other market data sources 51
10.6 Anonymity of the parties to a Publicly Reportable Security-Based Swap Transaction 52
10.6.1 Notional rounding and capping 52
11.0 Dispute Resolution 53
12.0 Chief Compliance Officer 53
12.1 CCO Designation 53
12.2 CCO Supervision 53
12.3 CCO Qualifications 54
13.0 KOR SBSDR system 55
13.1 Hours of Operation 55
13.2 Emergency policies and procedures 55
13.3 Systems Safeguards 56
13.3.1 Systems testing 56
13.3.2 Systems testing planning 56
13.4 Fees to use KOR SBSDR services 56
14.0 Disciplinary procedures 57
14.1 Violation of KOR SBSDR rules 57
14.2 Client Denial, Revocation, or Suspension 57

14.3 Restoring Client Access 58

0.1 Preamble

KOR Reporting Inc. (“KOR” or “KOR SDR”) and its affiliate, KOR Financial Inc.**,** are wholly owned subsidiaries of KOR US Holdings, Inc.. KOR Reporting Inc. operates a U.S. Security-Based Swap Data Repository (“SBSDR”). The KOR SBSDR is governed by the Securities and Exchange Commission (“SEC” or “Commission”).

KOR SDR is registered for and accepts data in the following Asset Classes under CFTC regulations: interest rates, credit default swaps, equities, foreign exchange and other commodities. KOR SBSDR is registered for and accepts data in the following Asset Classes under SEC regulations: credit default swaps and equities. To maintain its SBSDR and SDR registration, KOR shall continue to demonstrate substantial compliance with all applicable provisions of its orders and applicable requirements set forth in the Commodity Exchange Act (“CEA”) and Parts 40, 43, 45 and 49 of the CFTC Regulations and Regulation SBSR (17 CFR 242.900 through 242.909) and Rules 13n-1 through 13n-12 (17 CFR 240.13n-1 through 240.13n-12) of the SEC Regulations.

KOR’s SBSDR is required to provide Appropriate Domestic Regulators and Appropriate Foreign Regulators that have executed a confidentiality arrangement with the Commission, access to swap data maintained by KOR SBSDR within the scope of such Regulator's jurisdiction. There will be no notification to Clients on such occurrences. Notwithstanding, KOR SBSDR is not a “self-regulatory organization, and as such, KOR SBSDR’s role with respect to any such objectives or tasks will be limited to monitoring, screening and analyzing the SBSDR Data.

Unless necessary or appropriate to achieve the purposes of the Securities Exchange Act of 1934, as amended (the “Exchange Act”), KOR SBSDR shall avoid adopting any rule or taking any action that results in any unreasonable restraint of trade; or imposing any material anticompetitive burden on trading, clearing or reporting swaps.

KOR SBSDR’s Chief Compliance Office can be contacted using: compliance@korfinancial.com

1.0 Defined terms

1.1 KOR Specific terms

Term	Definition	Acronym
Administrative User	All Clients must indicate at least two Administrative Users. These Users manage all other User's access to the KOR system.	
Authorized Access Client	A Client that has been authorized to access other Client’s data, but not submit data on its behalf.	
Client	All-encompassing term for a company who has executed all applicable KOR Agreements and Addendums. Includes Reporting, 3rd Party Reporter, Verification, Integration, Authorized Access and Regulator Client types.	
Delegated Reporter	Related Entities and Third-Party Reporters are together referred to as Delegated Reporters.	
Integration Client	A Client registered to receive systems integration support for the purpose of supplying to their customers who will report and be charged fees by KOR SBSDR. Integration Clients access to KOR SBSDR is limited to the testing environment	
KOR SBSDR Technical Specification	Detailed information on the connection and integration to KOR SBSDR for submission, access and reports	
KOR SBSDR User Guide	Functional and operational information for the use of the SBSDR	
On Facility	Any swap executed on an execution facility (e.g., SEF, DCM, FBOT, NSE, SBSEF)	
Original security-based swap	An “original security-based swap” is defined as a swap that has been accepted for clearing by a clearing authority	
Regulator Client	Primary Regulator, Delegated Regulator, Appropriate Domestic Regulator or Foreign Regulator that has approved access to KOR SBSDR.	

Related Entity	Related Entity is a Client that is part of the same corporate family, where the shared parent has controlling interest, or is in a fiduciary relationship with the Reporting (Counterparty) Client.	
SBSDR Data	SBSDR Data means the specific data elements and information required to be reported to a security-based swap data repository or disseminated by a security-based swap data repository pursuant to SEC Regulations 17 CFR 242.900 through 242.909 and 17 CFR 240.13n-1 through 240.13n-12.	
SBSDR Regulations	Rules and regulations under 17 CFR 242.900 through 242.909 and 17 CFR 240.13n-1 through 240.13n-12.	
SBSDR User Interface	Web interface to access data, entity information and manage Users/access.	SBSDR UI
SBSDR Website	Public website where Clients and non-Clients can access any SBSDR public information as well as Agreements to become a Client.	
Security-Based Swap Data	Security-Based Swap Data means the specific data elements and information required to be reported to a security-based swap data repository pursuant to SEC Rules.	
Security-Based Swap Transaction and Pricing Data	Security-Based Swap Transaction and Pricing Data means the specific data elements and information required to be reported to a security-based swap data repository or publicly disseminated by a security-based swap data repository pursuant to SEC rules.	
Third-party Reporter Client	Company that has executed the KOR Universal Services Agreement and applicable Addendums but are not a counterparty or party to a swap. Reporting Side Clients must permission them to submit data on their behalf.	3PR
User	Person or system with SBSDR access at a Client	

	or Regulator	
Verification Client	A company who has executed the applicable KOR Agreement, but is not accessed to submit data, only view data or permission other Clients to submit or view data on their behalf.	

a. SEC Terms

Each “SEC Term” is incorporating by reference such term as defined under SEC rules. Terms used in §§ 242.900 through 242.909 that appear in Section 3 of the Exchange Act (15 U.S.C. 78c) have the same meaning as in Section 3 of the Exchange Act and the rules or regulations thereunder. In addition, for purposes of Regulation SBSR (§§ 242.900 through 242.909) , the following definitions shall apply:

Term	Definition	Acronym	Citation

Affiliate	Affiliate means any person that, directly or indirectly, controls, is controlled by, or is under common control with, a person.
	Affiliate of a security-based swap data repository means a person that, directly or indirectly, controls, is controlled by, or is under common control with the security-based swap data repository.
			242.900(a)
			240.13n-4(a)(1)
			240.13n-9(a)(1)

Asset class	Asset class means those security-based swaps in a particular broad category, including, but not limited to, credit derivatives and equity derivatives.		242.900(b)
			240.13n-5(a)(1)

Board	Board means the board of directors of the security-based swap data repository or a body performing a function similar to the board of directors of the security-based swap data repository.		240.13n-4(a)(2)
			240.13n-11(b)(1)

Branch ID	Branch ID means the UIC assigned to a branch or other unincorporated office of a participant.		242.900(d)
Broker ID	Broker ID means the UIC assigned to a person acting as a broker for a participant.		242.900(e)
Business day	Business day means a day, based on U.S. Eastern Time, other than a Saturday, Sunday, or a U.S. federal holiday.		242.900(f)
Clearing transaction	Clearing transaction means a security-based swap that has a registered clearing agency as a direct counterparty.		242.900(g)
Control	Control means, for purposes of §§ 242.900 through 242.909, the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract, or otherwise. A person is presumed to control another person if the person: a. Is a director, general partner or officer exercising executive responsibility (or having		

	similar status or functions);
	b. Directly or indirectly has the right to vote 25 percent or more of a class of voting securities or has the power to sell or direct the sale of 25 percent or more of a class of voting securities; or
	c. In the case of a partnership, has the right to receive, upon dissolution, or has contributed, 25 percent or more of the capital.
	Control (including the terms controlled by and under common control with) means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract, or otherwise. A person is presumed to control another person if the person:
	a. Is a director, general partner, or officer exercising executive responsibility (or having similar status or functions);
	b. Directly or indirectly has the right to vote 25 percent or more of a class of voting securities or has the power to sell or direct the sale of 25 percent or more of a class of voting securities; or
	c. In the case of a partnership, has the right to receive, upon dissolution, or has contributed, 25 percent or more of the capital.
			242.900(h)
			240.13n-4(a)(3)
			240.13n-9(a)(2)

Counterparty	Counterparty means a person that is a direct counterparty or indirect counterparty of a security-based swap.		242.900(i)
Counterparty ID	Counterparty ID means the UIC assigned to a counterparty to a security-based swap.		242.900(j)

Director	Director means any member of the board.		240.13n-4(a)(4)
			240.13n-11(b)(2)

Direct counterparty	Direct counterparty means a person that is a primary obligor on a security-based swap.		242.900(k)

Direct electronic access	Direct electronic access means access, which shall be in a form and manner acceptable to the Commission, to data stored by a security-based swap data repository in an electronic format and updated at the same time as the security-based swap data repository's data is updated so as to provide the Commission or any of its designees with the ability to query or analyze the data in the same manner that the security-based swap data repository can query or analyze the data.		242.900(l)
			240.13n-4(a)(5)

EDGAR Filer Manual	The term EDGAR Filer Manual means the current version of the manual prepared by the Commission setting out the technical format requirements for an electronic submission.		240.13n-11(b)(3) Rule 11 of Regulation S-T (17 CFR 232.11)
Exchange Act	Exchange Act means the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.), as amended.		242.900(m)
Execution agent ID	Execution agent ID means the UIC assigned to any person other than a broker or trader that facilitates the execution of a security-based swap on behalf of a direct counterparty.		242.900(n)

Foreign branch	Foreign branch means any branch of a U.S. bank if:
	a. The branch is located outside the United States;
	b. The branch operates for valid business reasons; and
	c. The branch is engaged in the business of banking and is subject to substantive banking regulation in the jurisdiction where located.
			242.900(o)
			240.3a71-3(a)(1)

Indirect counterparty	Indirect counterparty means a guarantor of a direct counterparty's performance of any obligation under a security-based swap such that the direct counterparty on the other side can exercise rights		

	of recourse against the indirect counterparty in connection with the security-based swap; for these purposes a direct counterparty has rights of recourse against a guarantor on the other side if the direct counterparty has a conditional or unconditional legally enforceable right, in whole or in part, to receive payments from, or otherwise collect from, the guarantor in connection with the security-based swap.		242.900(p)
Interactive Data File	The term Interactive Data File means the machine-readable computer code that presents information in eXtensible Business Reporting Language (XBRL) electronic format pursuant to § 232.405 and as specified by the EDGAR Filer Manual. When a filing is submitted using Inline XBRL as provided by § 232.405(a)(3), a portion of the Interactive Data File is embedded into a filing with the remainder submitted as an exhibit to the filing.		240.13n-11(b)(4) Rule 11 of Regulation S-T (17 CFR 232.11)
Life cycle event	Life cycle event means, with respect to a security-based swap, any event that would result in a change in the information reported to a registered security-based swap data repository under § 242.901(c), (d), or (i), including: An assignment or novation of the security-based swap; a partial or full termination of the security-based swap; a change in the cash flows originally reported; for a security-based swap that is not a clearing transaction, any change to the title or date of any master agreement, collateral agreement, margin agreement, or any other agreement incorporated by reference into the security-based swap contract; or a corporate action affecting a security or securities on which the security-based swap is based (e.g., a merger, dividend, stock split, or bankruptcy). Notwithstanding the above, a life cycle event shall not include the scheduled expiration of the security-based swap, a previously described and anticipated interest rate adjustment (such as a quarterly interest rate adjustment), or other event that does not result in any change to the contractual terms of the security-based swap.		242.900(q)

Market participant	Market participant means any person participating in the security-based swap market, including, but not limited to, security-based swap dealers, major security-based swap participants, and any other counterparties to a security-based swap transaction.		240.13n-4(a)(6)
			240.13n-9(a)(3)

Material change	Material change means a change that a chief compliance officer would reasonably need to know in order to oversee compliance of the security-based swap data repository.		240.13n-11(b)(5)
Material compliance matter	Material compliance matter means any compliance matter that the board would reasonably need to know to oversee the compliance of the security-based swap data repository and that involves, without limitation: a. A violation of the federal securities laws by the security-based swap data repository, its officers, directors, employees, or agents; b. A violation of the policies and procedures of the security-based swap data repository by the security-based swap data repository, its officers, directors, employees, or agents; or c. A weakness in the design or implementation of the policies and procedures of the security-based swap data repository.		240.13n-11(b)(6)

Nonaffiliated third party of a security-based swap data repository	Nonaffiliated third party of a security-based swap data repository means any person except:
	a. The security-based swap data repository;
	b. Any affiliate of the security-based swap data repository; or
	c. A person employed by a security-based swap data repository and any entity that is not the security-based swap data repository's affiliate (and “nonaffiliated third party” includes such entity that jointly employs the person).
			240.13n-4(a)(7)
			240.13n-9(a)(4)

Non-mandatory			

report	Non-mandatory report means any information provided to a registered security-based swap data repository by or on behalf of a counterparty other than as required by §§ 242.900 through 242.909.		242.900(r)
Nonpublic personal information	Nonpublic personal information means: a. Personally identifiable information that is not publicly available information; and b. Any list, description, or other grouping of market participants (and publicly available information pertaining to them) that is derived using personally identifiable information that is not publicly available information.		240.13n-9(a)(5)

Non-U.S. person	Non-U.S. person means a person that is not a U.S. person.		242.900(s)
			240.13n-12(a)(1)

Official filing	The term official filing means any filing that is received and accepted by the Commission, regardless of filing medium and exclusive of header information, tags and any other technical information required in an electronic filing; except that electronic identification of investment company type and inclusion of identifiers for series and class (or contract, in the case of separate accounts of insurance companies) as required by rule 313 of Regulation S-T (§ 232.313) are deemed part of the official filing.		240.13n-11(b)(7) Rule 11 of Regulation S-T (17 CFR 232.11)
Parent	Parent means a legal person that controls a participant.		242.900(t)
Participant	Participant, with respect to a registered security-based swap data repository, means: a. A counterparty, that meets the criteria of § 242.908(b), of a security-based swap that is reported to that registered security-based swap data repository to satisfy an obligation under § 242.901(a); b. A platform that reports a security-based swap		

	to that registered security-based swap data repository to satisfy an obligation under § 242.901(a); c. A registered clearing agency that is required to report to that registered security-based swap data repository whether or not it has accepted a security-based swap for clearing pursuant to § 242.901(e)(1)(ii); or d. A registered broker-dealer (including a registered security-based swap execution facility) that is required to report a security-based swap to that registered security-based swap data repository by § 242.901(a).		242.900(u)
Personally identifiable information	Personally identifiable information means any information: a. A market participant provides to a security-based swap data repository to obtain service from the security-based swap data repository; b. About a market participant resulting from any transaction involving a service between the security-based swap data repository and the market participant; or The security-based swap data repository obtains about a market participant in connection with providing a service to that market participant.		240.13n-9(a)(6)

Person associated with a security-based swap data repository	Person associated with a security-based swap data repository means:
	a. Any partner, officer, or director of such security-based swap data repository (or any person occupying a similar status or performing similar functions);
	b. Any person directly or indirectly controlling, controlled by, or under common control with such security-based swap data repository; or
	c. Any employee of such security-based swap data repository.
			240.13n-4(a)(8)
			240.13n-9(a)(7)

Platform	Platform means a national securities exchange or security-based swap execution facility that is registered or exempt from registration.		242.900(v)
Platform ID	Platform ID means the UIC assigned to a platform on which a security-based swap is executed.		242.900(w)
Position	Position means the gross and net notional amounts of open security-based swap transactions aggregated by one or more attributes, including, but not limited to, the: a. Underlying instrument, index, or reference entity; b. Counterparty; c. Asset class; d. Long risk of the underlying instrument, index, or reference entity; and e. Short risk of the underlying instrument, index, or reference entity.		240.13n-5(a)(2)
Post-trade processor	Post-trade processor means any person that provides affirmation, confirmation, matching, reporting, or clearing services for a security-based swap transaction.		242.900(x)
Pre-enactment security-based swap	Pre-enactment security-based swap means any security-based swap executed before July 21, 2010 (the date of enactment of the Dodd-Frank Act (Pub. L. 111-203, H.R. 4173)), the terms of which had not expired as of that date.		242.900(y)
Price	Price means the price of a security-based swap transaction, expressed in terms of the commercial conventions used in that asset class.		242.900(z)
Product	Product means a group of security-based swap contracts each having the same material economic terms except those relating to price and size.		242.900(aa)
Product ID	Product ID means the UIC assigned to a product.		242.900(bb)

Publicly disseminate	Publicly disseminate means to make available through the Internet or other electronic data feed that is widely accessible and in machine-readable electronic format.		242.900(cc)
Registered clearing agency	Registered clearing agency means a person that is registered with the Commission as a clearing agency pursuant to section 17A of the Exchange Act (15 U.S.C. 78q-1) and any rules or regulations thereunder.	CA	242.900(ee)
Registered security-based swap data repository	Registered security-based swap data repository means a person that is registered with the Commission as a security-based swap data repository pursuant to section 13(n) of the Exchange Act (15 U.S.C. 78m(n)) and any rules or regulations thereunder.	SBSDR	242.900(ff)
Reporting side	Reporting side means the side of a security-based swap identified by § 242.901(a)(2).		242.900(gg)
Senior officer	Senior officer means the chief executive officer or other equivalent officer.		240.13n-11(b)(8)
Side	Side means a direct counterparty and any guarantor of that direct counterparty's performance who meets the definition of indirect counterparty in connection with the security-based swap.		242.900(hh)
Tag	The term tag means an identifier that highlights specific information to EDGAR that is in the format required by the EDGAR Filer Manual.		240.13n-11(b)(9) Rule 11 of Regulation S-T (17 CFR 232.11)
Time of execution	Time of execution means the point at which the counterparties to a security-based swap become irrevocably bound under applicable law.		242.900(ii)
Trader ID	Trader ID means the UIC assigned to a natural person who executes one or more security-based swaps on behalf of a direct counterparty.		242.900(jj)

Trading desk	Trading desk means, with respect to a counterparty, the smallest discrete unit of organization of the participant that purchases or sells security-based swaps for the account of the participant or an affiliate thereof.		242.900(kk)
Trading desk ID	Trading desk ID means the UIC assigned to the trading desk of a participant.		242.900(ll)
Transaction data	Transaction data means all information reported to a security-based swap data repository pursuant to the Act and the rules and regulations thereunder, except for information provided pursuant to Rule 906(b) of Regulation SBSR (17 CFR 242.906(b)).		240.13n-5(a)(3)
Transaction ID	Transaction ID means the UIC assigned to a specific security-based swap transaction.		242.900(mm)
Transitional security-based swap	Transitional security-based swap means a security-based swap executed on or after July 21, 2010, and before the first date on which trade-by-trade reporting of security-based swaps in that asset class to a registered security-based swap data repository is required pursuant to §§ 242.900 through 242.909.		242.900(nn)
Ultimate parent	Ultimate parent means a legal person that controls a participant and that itself has no parent.		242.900(oo)
Ultimate parent ID	Ultimate parent ID means the UIC assigned to an ultimate parent of a participant.		242.900(pp)
Unique Identification Code (UIC)	Unique Identification Code or UIC means a unique identification code assigned to a person, unit of a person, product, or transaction.	UIC	242.900(qq)

United States	United States *means the United States of America, its territories and possessions, any State of the United States, and the District of Columbia.*		242.900(rr)
			240.3a71-3(a)(5)

U.S. person	U.S. person (i) Except as provided in paragraph (a)(4)(iii) of this section, *U.S. person* means any person that is: (A) A natural person resident in the United States;		

	(B) A partnership, corporation, trust, investment vehicle, or other legal person organized, incorporated, or established under the laws of the United States or having its principal place of business in the United States;
	(C) An account (whether discretionary or non-discretionary) of a U.S. person; or
	(D) An estate of a decedent who was a resident of the United States at the time of death.
	(ii) For purposes of this section, *principal place of business* means the location from which the officers, partners, or managers of the legal person primarily direct, control, and coordinate the activities of the legal person. With respect to an externally managed investment vehicle, this location is the office from which the manager of the vehicle primarily directs, controls, and coordinates the investment activities of the vehicle.
	(iii) The term *U.S. person* does not include the International Monetary Fund, the International Bank for Reconstruction and Development, the Inter-American Development Bank, the Asian Development Bank, the African Development Bank, the United Nations, and their agencies and pension plans, and any other similar international organizations, their agencies and pension plans.
	(iv) A person shall not be required to consider its counterparty to a security-based swap to be a U.S. person if such person receives a representation from the counterparty that the counterparty does not satisfy the criteria set forth in paragraph (a)(4)(i) of this section, unless such person knows or has reason to know that the representation is not accurate; for the purposes of this final rule a person would have reason to know the representation is not accurate if a reasonable person should know, under all of the facts of which the person is aware, that it is not accurate.
			242.900(ss)
			240.3a71-3(a)(4)
			240.13n-12(a)(2)

Widely accessible	Widely accessible, as used in paragraph (cc) of this section, means widely available to users of the		

	information on a non-fee basis.		242.900(tt)

2.0 No action relief

KOR SBSDR's application of SEC Rules and its SBSDR is consistent with the no action relief provisions set out in the adopting release "Cross-Border Application of Certain Security-Based Swap Requirements" ("Cross-Border Release"). KOR is relying on the provisions in this Cross-Border Release. This relief will remain in effect until the earlier of (i) four years following the applicable Reporting Compliance Date, (as defined below) or (ii) 12 months following notice by the Commission that the relief will expire. For these purposes, the applicable "Reporting Compliance Date" means, with respect to an asset class, the first Monday that is the later of (1) six months after the date on which the first SBSDR that can accept transaction reports in that asset class registers with the Commission, or (2) November 6, 2021. SBSDRs are not required to adhere to any security information processor provisions of Section 11A(b) of the Exchange Act. No information, therefore, is included in this Rulebook related to the duties of a securities information processor.

KOR represents that it is provisionally registered with the Commodity Futures Exchange Commission ("CFTC") as a swap data repository ("SDR") and is in compliance with applicable requirements under the CFTC reporting rules applicable to a registered SDR. KOR intends to rely on the Commission's position outlined in the Cross-Border Release for applicable reporting rules and SBSDR duties for the period set forth.

3.0 Corporate structure

3.1 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.

3.1.1 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.

3.2 Board membership and structure

3.2.1 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.

3.2.2 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.

Reference SEC Rule 240.13n-4(c)(2)(iii).

3.2.3 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.

3.2.4 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.

3.2.5 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.

4.0 Client access to data

4.1 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^1 as published by KOR SBSDR; 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.

References SEC Rule(s) 13n-4(c)(1).

Technical Specifications^1: The KOR SBSDR Technical Specifications include all CFTC Technical Specifications in addition to KOR SBSDR's additional fields and validations.

4.2 Client Rules & Applicable Law

By entering into the KOR USA, each Client agrees to be bound by the terms of the USA, this 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.

4.3 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.

4.4 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.

4.5 Users

4.5.1 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.

4.5.2 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:^2

a. Central counterparty
b. Clearing member
c. Counterparty 1
d. Counterparty 2
e. Submitter identifier
f. Reporter identifier^3
g. Counterparty 1 Agent^4
h. Counterparty 2 Agent^5

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.

fields:^2: Fields are defined in the KOR Technical Specifications.

Reporter identifier^3: This 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.

Counterparty 1 Agent^4: 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.

Counterparty 2 Agent^5: 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.

4.5.3 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.

4.5.4 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.

5.0 Unique Identifiers

5.1 Coded information^6

Coded information^6: 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.

5.1.1 Assigning UICs for entities^7

KOR SBSDR endorses the use of the Legal Entity Identifier^8 ("LEI").^9, 10, 11

Where an individual is not eligible for an LEI they should be reported using a Natural Person Identifier.

References: SEC Rule(s) § 242.903(a).

Assigning UICs for entities^7: KOR will not create UICs per the SEC Cross-Border Release no action: With respect to Rule 907(a)(5) of Regulation SBSR, if a registered SDR does not have policies and procedures for assigning UICs.

Legal Entity Identifier^8: https://www.gleif.org/en

^9 KOR will not support fields that would contain information that is outside of an LEI or Natural Person Identifier UIC per the SEC Cross-Border Release no action: With respect to Rule 907(a)(5) of Regulation SBSR, if a registered SDR does not have policies and procedures for assigning UICs.

^10: KOR will not collect ultimate parent and affiliate information per the SEC Cross-Border Release no action: With respect to Rule 906(b) of Regulation SBSR, if a registered SDR does not collect ultimate parent and affiliate information from its participants.'

^11: SEC Cross-Border Release no action: With respect to Rule 907(a)(6) of Regulation SBSR, if a registered SDR does not have policies and procedures for obtaining from its participants information about each participant's ultimate parent and affiliates.

5.1.2 Assigning transaction ID

KOR SBSDR endorses the use of the Unique Trade Identifier^12 ("UTI") methodology. Until UTIs are mandated by the CFTC and/or SEC for reporting, KOR will accept Unique Swap Identifiers^13 ("USIs") per the CFTC specifications.
KOR SBSDR will not assign transaction identifiers.

References: SEC Rule(s) § 242.901(g).

Trade Identifier^12: https://www.leiroc.org/publications/gls/roc_20170901.pdf

Swap Identifiers^13:
https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/dfsubmission/usidatastanda

5.1.3 Public dissemination of coded information

Until the UPI is available, KOR will not use coded information for public dissemination. ^14

References: SEC Rule(s) § 242.903(b).

public dissemination. ^14: SEC Cross-Border Release no action: With respect to Rule 903(b), a registered SDR permits the reporting or public dissemination of SBS transaction information that includes codes in place of certain data elements even if the information necessary to interpret such codes is not widely available to users of the information on a non-fee basis.

5.2 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.

5.2.1 UTI Creation format

The Market Participant designated to generate the UTI shall generate and assign the UTI at, or As Soon As Technologically Practicable (ASATP) following, the time of execution of the swap, and prior to the reporting of required Security-Based Swap Data. The unique trade identifier shall consist of a single data element with a maximum length of 52 characters that contains two components:

a. The legal entity identifier of the Market Participant who generated the UTI^15; and

b. An uppercase alphanumeric code generated and assigned to that swap by the automated systems of the entity that generated the UTI.

UTI^15: This may be the LEI of the Third-party service provider.

5.2.2 UTI Transmission

The Market Participant designated to generate the UTI shall transmit the unique trade identifier electronically as follows:

a. To the Security-Based Swap Data Repository to which the swap is reported as part of all submissions.

b. To each counterparty to the security-based swap, ASATP after execution of the security-based swap.

c. To the Clearing Agency, if any, to which the swap is submitted for clearing, as part of the required swap creation data transmitted to the CA for clearing purposes.

d. To the agent in the case of a post-allocation swap.

5.2.3 UTI Creation Entity

The UTI Technical Guidance^16 should be followed to determine which entity generates the UTI.

Technical Guidance^16: https://www.bis.org/cpmi/publ/d158.pdf

5.3 Legal Entity Identifiers (LEI)

Each party to a security-based swap that is eligible to receive a legal entity identifier shall obtain, maintain, and be identified in all KOR SBSDR reporting by a single legal entity identifier.

The legal entity identifier used in all record keeping and all Security-Based Swap Data reporting shall be issued under, and shall conform to, ISO Standard 17442, Legal Entity Identifier (LEI), issued by the International Organization for Standardization.
During the Client onboarding process, KOR SBSDR requires the Client provide their LEI code and legal name that aligns with GLEIF along with additional information such as entity type (e.g., Security-Based Swap Dealer, Security-Based Major Swap Participant).

5.3.1 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.

5.4 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.

5.4.1 KOR SBSDR’s temporary unique product identifier system

KOR will use the fields and guidance as published by CPMI and IOSCO in the Technical Guidance on the Harmonization of the Unique Product Identifier. Until the UPI is available for use, KOR will attempt to follow the public standards and guidance regarding the UPI creation in order to migrate to the UPI more seamlessly when available. Clients will have access to all allowed data values for the product fields.

Before executing and reporting a Security-Based Swap the Client must verify the applicable product data values exist in the KOR product schema, if they do not, the Client must contact KOR and provide the required new values and their public source or other pertinent details for reference to the KOR Client Support group (support@korfinancial.com) a minimum of 48 business hours before reporting is required. Failure to do so could result in late reporting.

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

6.1 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^18

References: SEC Rule(s) §242.901(a).

follows^18: Clients may apply the SEC Cross-Border Release no action: With respect to Rule 901(a) of Regulation SBSR if a person with a duty to report an SBS transaction (or a duty to participate in the selection of the reporting side) under Rule 901(a) does not report the transaction (or does not participate in the selection of the reporting side) because, under the swap reporting rules in force at the time of the transaction, a different person (or no person) would have the duty to report a comparable swap transaction.

Notwithstanding the above, the Commission's position with respect to Rule 901(a) of Regulation SBSR does not extend to instances where a transaction falls within Rule 901(a)(2)(ii)(E) and one or both sides is relying on the exception to the de minimis counting requirement for ANE transactions (i.e., is a “relying entity”). The Commission expects that a foreign dealing entity that is a relying entity would utilize staff of an affiliated U.S. registered SBS dealer or broker-dealer to report an ANE transaction. Furthermore, the Commission's position with respect to Rule 902(a) of Regulation SBSR does not extend to: (1) A covered inter-dealer security-based swap transaction that at least one side of the transaction arranges, negotiates, or executes in reliance on the exception in Rule 3a71-3(d); or (2) a security-based swap transaction between a relying entity and a registered SBS dealer (whether or not it is a U.S. person). All other aspects of the Commission's position extend to the transactions described in this paragraph.

6.1.1 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).

References: SEC Rule(s) § 242.901(a)(1).

6.1.2 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.

References: SEC Rule(s) § 242.901(a)(2).

6.1.3 Clearing transactions

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

References: SEC Rule(s) § 242.901(a)(2)(i).

6.1.4 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).

References: SEC Rule(s) § 242.901(a)(2)(ii), 242.901(a)(2)(ii)(A), 242.901(a)(2)(ii)(B), 242.901(a)(2)(ii)(C), 242.901(a)(2)(ii)(D), 242.901(a)(2)(ii)(E), 242.901(a)(2)(ii)(E)(1), 242.901(a)(2)(ii)(E)(2), 242.901(a)(2)(ii)(E)(3), and 242.901(a)(2)(ii)(E)(4).

6.2 Notification to registered clearing agency

A person who, under SEC Rule(s) § 242.901(a)(1) or (a)(2)(ii), has a duty to report a security-based swap that has been submitted to clearing at a registered clearing agency shall promptly provide that registered clearing agency with the transaction ID of the submitted security-based swap and the identity of the registered security-based swap data repository to which the transaction will be reported or has been reported.

References: SEC Rule(s) § 242.901(a)(3).

6.3 Interim timeframe for reporting

The reporting timeframe for SEC Rule(s) § 242.901(c) and (d) shall be 24 hours after the time of execution (or acceptance for clearing in the case of a security-based swap that is subject to regulatory reporting and public dissemination solely by operation of § 242.908(a)(1)(ii)), or, if 24 hours after the time of execution or acceptance, as applicable, would fall on a day that is not a business day, by the same time on the next day that is a business day.

Late reporting is based on the KOR SBSDR's calculated Original Submission Timestamp vs. the Execution Timestamp. The Original Submission Timestamp is calculated based on when the swap is first received by the KOR SBSDR and has passed all KOR SBSDR validations. Business Days means the twenty-four-hour day, on all days except Saturdays, Sundays, and US Federal holidays. Eastern time is used for business hours. Swaps with an “Event type” of “PORT” are excluded from this timeline for new submissions.

References: SEC Rule(s) § 242.901(j).

6.4 Trade information

The reporting side shall report the primary and secondary trade information within the timeframe specified in under SEC Rule(s) § 242.901(j). The KOR Technical Specifications define how to report the required information regarding the security-based swap.^19, 20, 21

References: SEC Rule(s) § 242.901(c), 242.901(c)(1), 242.901(c)(1)(i), 242.901(c)(1)(ii), 242.901(c)(1)(iv), 242.901(c)(1)(v), 242.901(c)(2), 242.901(c)(3), 242.901(c)(4), 242.901(c)(5), 242.901(c)(6), 242.901(c)(7), 242.901(d), 242.901(d)(1), 242.901(d)(2), 242.901(d)(3), 242.901(d)(4), 242.901(d)(5), 242.901(d)(6), 242.901(d)(7), 242.901(d)(8), 242.901(d)(9), and 242.901(d)(10).

swap.^19, 20, 21: KOR SBSDR has applies the following when defining the required fields in the KOR Technical Specifications - SEC Cross-Border Release no action: With respect to Rules 901(c)(2)-(7) and 901(d) of Regulation SBSR, if a person with a duty to report a data element of an SBS transaction, as required by any provision of Rules 901(c)(2)-(7) and 901(d), does not report that data element because the swap reporting rules in force at the time of the transaction do not require that data element to be reported.

KOR SBSDR has applies the following when defining the required fields in the KOR Technical Specifications - SEC Cross-Border Release no action: With respect to Rule 907(a)(1) of Regulation SBSR, if a registered SDR does not enumerate in its policies and procedures for reporting transaction information one or more specific data elements that are required by Rule 901(c) or 901(d) of Regulation SBSR, because such data element(s) are not required under the swap reporting rules, except that the registered SDR's policies and procedures must set out how a participant must identify the SBS and any security underlying the SBS and thereby comply with Rule 901(c)(1).

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.

6.5 Reporting of life cycle events

A life cycle event, and any adjustment due to a life cycle event, that results in a change to information previously reported pursuant to SEC Rule(s) § 242.901(c), (d), or (i) shall be reported by the reporting side, except that the reporting side shall not report whether or not a security-based swap has been accepted for clearing.^22

Clients must follow the KOR Technical Specifications to submit life-cycle event data. For open swaps, all life-cycle event data submissions must include all applicable fields and be submitted according to the format and validations prescribed by the KOR SBSDR at the time of submission and not at the time the trade was initially executed.
Clients shall not submit life cycle event data messages that do not update any KOR SBSDR fields or correct a previous submission.

References: SEC Rule(s) § 242.901(e) and 242.901(e)(1)(i).

clearing.^22: KOR SBSDR has applies the following when defining how to report life cycle events in the KOR SBSDR Technical Specifications and User Guide. These align with the CFTC rules as amended and published on Nov. 25, 2020 - SEC Cross-Border Release no action: With respect to Rule 901(e) of Regulation SBSR, if a person does not report a life cycle event of an SBS transaction in a manner consistent with Rule 901(e) and the person acts instead in a manner consistent with the swap reporting rules for the reporting of life cycle events that are in force at the time of the life cycle event.

6.5.1 Acceptance for clearing

A registered clearing agency that has accepted a security-based swap for clearing shall submit a termination message to the original swap per the KOR Technical Specifications^23.

References: SEC Rule(s) § 242.901(e)(1)(ii).

Specifications^23: Per SEC Cross-Border Release no action: With respect to Rule 907(a)(3) of Regulation SBSR, if a registered SDR does not enumerate in its policies and procedures for handling life cycle events provisions that are not required under swap reporting rules that pertain to the reporting of life cycle events. KOR has defined the message to terminate an accepted swap for clearing, but as the CFTC rules have no message requirement for a DCO to report when a swap has not been accepted to clearing, there is no message defined for the CA to report.

6.5.2 Life cycle reporting timeline

All reports of life cycle events and adjustments due to life cycle events shall, within the timeframe specified in SEC Rule(s) § 242.901(j), be reported to the entity to which the original security-based swap transaction will be reported or has been reported and shall include the transaction ID of the original transaction.

6.5.3 Interim timeframe for reporting

The reporting timeframe for SEC Rule(s) § 242.901(e) of this section shall be 24 hours after the occurrence of the life cycle event or the adjustment due to the life cycle event.

References: SEC Rule(s) § 242.901(e)(2).

6.6 Format of reported information.

A person having a duty to report shall electronically transmit the information required under SEC Rule(s) § 242.901 in a format required by the registered security-based swap data repository to which it reports. KOR has published the KOR Technical Specifications which outlines these requirements.

References: SEC Rule(s) § 242.901(h).

6.7 Reporting of pre-enactment and transitional security-based swaps

With respect to any pre-enactment security-based swap or transitional security-based swap in a particular asset class, and to the extent that information about such transaction is available, the reporting side shall report all of the information required by SEC Rule(s) § 242.901(c) and (d) to a registered security-based swap data repository that accepts security-based swaps in that asset class and indicate whether the security-based swap was open as of the date of such report.

KOR accepts pre-enactment and transitional security-based swaps. The Client must indicate when a security-based swap is a pre-enactment or transitional security-based swaps. Any swaps that are still open must be reported to the current and full KOR SBSDR Technical Specifications. For closed pre-enactment or transitional security-based swaps the KOR SBSDR Technical Specifications defines minimum submission criteria.

References: SEC Rule(s) § 242.901(i).

6.8 Other duties of participants

6.8.1 Policies and procedures to support reporting compliance

Each participant of a registered security-based swap data repository that is a registered security-based swap dealer, registered major security-based swap participant, registered clearing agency, platform, or registered broker-dealer (including a registered security-based swap execution facility) that becomes a participant solely as a result of making a report to satisfy an obligation under SEC Rule § 242.901(a)(2)(ii)(E)(4) shall establish, maintain, and enforce written policies and procedures that are reasonably designed to ensure that it complies with any obligations to report information to a registered security-based swap data repository in a manner consistent with SEC Rule(s) §§ 242.900 through 242.909. Each such participant shall review and update its policies and procedures at least annually.

References: SEC Rule(s) § 242.906(c).

6.9 Cross-border matters

6.9.1 Application of Regulation SBSR to cross-border transactions

The Reporting Side has an obligation to report a public dissemination message to KOR when a security-based swap is subject to public dissemination. KOR shall only publicly disseminate messages determined to be applicable for public dissemination by the Reporting Side and as such submitted as a KOR public dissemination message per the KOR Technical Specifications. A security-based swap shall be subject to regulatory reporting and public dissemination if:

a. There is a direct or indirect counterparty that is a U.S. person on either or both sides of the transaction;

b. The security-based swap is accepted for clearing by a clearing agency having its principal place of business in the United States;

c. The security-based swap is executed on a platform having its principal place of business in the United States;

d. The security-based swap is effected by or through a registered broker-dealer (including a registered security-based swap execution facility); or

e. The transaction is connected with a non-U.S. person's security-based swap dealing activity and is arranged, negotiated, or executed by personnel of such non-U.S. person located in a U.S. branch or office, or by personnel of an agent of such non-U.S. person located in a U.S. branch or office.

A security-based swap that is not included within the above shall be subject to regulatory reporting but not public dissemination if there is a direct or indirect counterparty on either or both sides of the transaction that is a registered security-based swap dealer or a registered major security-based swap participant. The reporting side must represent this in the field “Exempt Related Public Message” per the KOR Technical Specifications.

References: SEC Rule(s) §242.908(a), 242.908(a)(1), 242.908(a)(1)(i), 242.908(a)(1)(ii), 242.908(a)(iii), 242.908(a)(iv), 242.908(a)(v), and 242.908(a)(2).

6.9.2 Limitation on obligations

Notwithstanding any other provision of §§ 242.900 through 242.909, a person shall not incur any obligation under §§ 242.900 through 242.909 unless it is:

a. A U.S. person;

b. A registered security-based swap dealer or registered major security-based swap participant;

c. A platform;

d. A registered clearing agency; or

e. A non-U.S. person that, in connection with such person's security-based swap dealing activity, arranged, negotiated, or executed the security-based swap using its personnel located in a U.S. branch or office, or using personnel of an agent located in a U.S. branch or office.

References: SEC Rule(s) §242.908(b), 242.908(b)(1), 242.908(b)(2), 242.908(b)(3), 242.908(b)(4), and 242.908(b)(5).

6.9.3 Substituted Compliance

Compliance with the regulatory reporting and public dissemination requirements in sections 13(m) and 13A of the Act (15 U.S.C. 78m(m) and 78m-1), and the rules and regulations thereunder, may be satisfied by compliance with the rules of a foreign jurisdiction that is the subject of a Commission order described in SEC Rule §242.908(c)(2) , provided that at least one of the direct counterparties to the security-based swap is either a non-U.S. person or a foreign branch.

In order for a reporting side to apply substituted compliance they SEC must first make a substituted compliance determination per SEC Rule §242.908(c)(2).

References: SEC Rule(s) §242.908(c)(1) and 242.908(c)(2).

6.10 Life cycle event data reporting for security-based original swaps

For each original security-based swap^24 the CA shall report required life cycle event data, including terminations, electronically to the Security-Based Swap Data Repository to which the security-based swap that was accepted for clearing was reported. Such required swap life cycle event data shall be accepted and recorded by KOR SBSDR when KOR SBSDR possesses the original security-based swap report.

The CA that accepted the security-based swap for clearing shall report all life-cycle event data electronically to a Security-Based Swap Data Repository not later than the end of the next Business Day following the day that any life-cycle event occurs with respect to the security-based swap.

In addition to all other required security-based swap data, life-cycle event data shall include all of the following:

a. The legal entity identifier of the Security-Based Swap Data Repository to which all required swap creation data for each clearing security-based swap was reported by the CA;
b. The unique trade identifier of the original security-based swap that was replaced by the clearing security-based swaps; and
c. The unique trade identifier of each clearing security-based swap that replaces a particular original security-based swap.

The KOR Technical Specifications defines the format of the original swap termination message.

swap^24 Original securities-based swap definition comes from the CFTC Rule 45.1(a) and means a swap that has been accepted for clearing by a clearing authority.

6.11 Third-party facilitation of data reporting

Registered entities and Reporting Sides required to report required securities-based swap data, while remaining fully responsible for reporting, may contract with Delegated Reporters to facilitate reporting.

6.12 Change of Security-Based Swap Data Repository

A Reporting Side may change the Securities-Based Swap Data Repository to which Security-Based Swap Transaction and Pricing Data and Security-Based Swap Data is reported.

6.12.1 SBSDR Porting: Notifications

At least five Business Days prior to changing the Securities-Based Swap Data Repository to which the Reporting Side reports Security-Based Swap Transaction and Pricing Data and Security-Based Swap Data for a security-based swap, the Reporting Side shall provide notice of such change to the other counterparty to the security-based swap, the Securities-Based Swap Data Repository to which Security-Based Swap Transaction and Pricing Data and Swap Data is currently reported, and the Securities-Based Swap Data Repository to which Security-Based Swap Transaction and Pricing Data and Security-Based Swap Data will be reported going forward. Such notification shall include the unique trade identifier of the security-based swap and the date on which the

Reporting Side will begin reporting such Security-Based Swap Transaction and Pricing Data and Security-Based Swap Data to a different Securities-Based Swap Data Repository.

6.12.2 SBSDR Porting: Procedure

After providing the required notifications, the Reporting Side shall follow KOR SBSDR's procedure as defined in the KOR SBSDR Rulebook, Technical Specifications, and User Guide to complete the change of Securities-Based Swap Data Repository.
The Reporting Side shall report the change of Securities-Based Swap Data Repository to the Securities-Based Swap Data Repository to which the Reporting Side is currently reporting Security-Based Swap Transaction and Pricing Data and Security-Based Swap Data as a life-cycle event.

On the same day that the Reporting Side reports required security-based swap data, the Reporting Side shall also report the change of Securities-Based Swap Data Repository to the Securities-Based Swap Data Repository to which Security-Based Swap Transaction and Pricing Data and Security-Based Swap Data will be reported going forward as a life-cycle event for such security-based swap. The required security-based swap data report shall identify the security-based swap using the same unique trade identifier used to identify the security-based swap at the previous Securities-Based Swap Data Repository.
Thereafter, all required security-based swap data, and required life-cycle event data for the security-based swap shall be reported to the same Securities-Based Swap Data Repository, unless the Reporting Side for the security-based swap makes another change to the Securities-Based Swap Data Repository to which such data is reported.

6.12.3 Changing Security-Based Swap Data Repository to KOR SBSDR

In order to port in swaps to KOR SBSDR:

a. At least five Business Days prior to porting into KOR SBSDR, the Client must provide notification in writing to KOR SBSDR of their intention to port in (support@korfinancial.com). Such notification shall include:
    i. The UTIs of the security-based swaps porting;
    ii. Planned porting date; and
    iii. Indication if the Client is porting all security-based swaps or only open security-based swaps.
a. Execute of the KOR Universal Services Agreement and applicable Addendums.
b. Administrative User must set up all User access.

c. Client must complete testing including the porting in of applicable security-based swaps in a non-production environment.

d. Client must complete all steps and port out security-based swaps from their current SBSDR on the same date security-based swaps are ported into KOR SBSDR.

e. All ported in security-based swaps shall be reported with [Action type] = ‘NEWT’ and [Event type] = ‘PORT’. Note that the transaction is reported using the same UTI and same execution timestamp.

  i. KOR only accept open security-based swaps for porting in by a Client.

  ii. All security-based swaps must be the current KOR Technical Standards.

  iii. All security-based swaps shall be reported in their current state.

6.12.4 Changing Security-Based Swap Data Repository out of KOR SBSDR

In order to port out security-based swaps from KOR SBSDR:

a. At least five Business Days prior to porting out of KOR SBSDR, the Client must provide notification in writing to KOR SBSDR of their intention to port out (support@korfinancial.com). Such notification shall include:

  i. The UTIs of the security-based swaps porting;

  ii. Planned porting date; and

  iii. Indication if the Client is porting all security-based swaps or only open security-based swaps.

a. Prior to the date the Client is porting out data, the Client must test their port out messages in a KOR SBSDR non-production environment.

b. For all security-based swaps that are being ported out, the Reporting Side submits a continuation data report that includes the field values: [Action type] = ‘PRTO’, [Event type] = ‘PORT’ and [New SBSDR identifier] = ‘LEISDR2’. This three-value combination is an indication that this transaction (UTI) will no longer be reported, effectively removing the active transaction from KOR SBSDR.

c. The Client must verify all open security-based swaps have been ported out and all open errors resolved.

7.0 Client data reporting standards

7.1 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 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.

8.0 Correction of errors in security-based swap information

8.1 Duty to correct

Any counterparty or other person having a duty to report a security-based swap that discovers an error in information previously reported pursuant to SEC Rule(s) §§ 242.900 through 242.909 shall correct such error in accordance with the following procedures:

a. If a person that was not the reporting side for a security-based swap transaction discovers an error in the information reported with respect to such security-based swap, that person shall promptly notify the person having the duty to report the security-based swap of the error; and

b. If the person having the duty to report a security-based swap transaction discovers an error in the information reported with respect to a security-based swap, or receives notification from a counterparty of an error, such person shall promptly submit to the entity to which the security-based swap was originally reported an amended report pertaining to the original transaction report. If the person having the duty to report reported the initial transaction to a registered security-based swap data repository, such person shall submit an amended report to the registered security-based swap data repository in a manner consistent with the policies and procedures contemplated by SEC Rule(s) § 242.907(a)(3).

References SEC Rule(s): §242.905, 242.905(a), 242.905(a)(1), 242.905(a)(2).

8.2 Form and manner for error correction

A Reporting Side shall conform to KOR SBSDR’s technical specifications created for the correction of errors.

8.2.1 Non-Reporting parties

Any non-Reporting Side that by any means becomes aware of any error in the Security-Based Swap Data for a security-based swap to which it is the non-Reporting Side, shall notify the Reporting Side for the security-based swap of the error ASATP after discovery. If the non-Reporting Side does not know the identity of the Reporting Side, the non-Reporting Side shall notify the Platform where the security-based swap was executed of the error ASATP after discovery.

8.2.2 Exception

The requirements to correct errors only apply to errors in Security-Based Swap Data relating to security-based swaps for which the record retention period under SEC Rule § 240.13n-5(b)(4) has not expired as of the time the error is discovered. If a Client attempts to submit a security-based swap that is past the retention period, the message shall fail KOR SBSDR validations.

8.3 Verification that Security-Based Swap Data is complete and accurate

The Security-Based Swap Data Repository shall verify the accuracy and completeness of Security-Based Swap Data that it receives from Clients.

Each Reporting Side shall verify that there are no errors in the Security-Based Swap Data for all open security-based swaps that the Reporting Side reported, or was required to report, to a Security-Based Swap Data Repository.

KOR SBSDR shall provide Clients with a positive acknowledgement (“ACK”) or negative acknowledgement (“NACK”) for all messages submitted to the KOR SBSDR including a detailed error message for all NACKS that identifies what validations failed. It is the duty of the Client to monitor and correct these errors. Clients will have access to a report of all open error messages that shall be reviewed and resolved ASATP. If a message was submitted in error and failed validations, the Client must correct and resubmit the message until it passes all validations per the KOR Technical Specifications.

8.3.1 Method of verification

KOR SBSDR shall provide an open security-based swaps report to all Clients and their Delegated Reporters or Authorized Access Clients when applicable. This report will provide the User with a view of the most recent validated and accepted open security-based swaps for which they have access for each field that was required to be reported per SEC rules where the Client is the Reporting Side. This information will allow Clients to successfully perform Security-Based Swap Data verification.

Each Reporting Side should utilize this mechanism for verification. The Client should compare all Security-Based Swap Data in the open security-based swaps verification report with all Security-Based Swap Data contained in the Reporting Side's internal books and records for each security-based swap, to verify that there are no errors in the relevant Security-Based Swap Data maintained by the Security-Based Swap Data Repository. In the event the Client identifies an error, including but not limited to: (1) an invalid field value, (2) a missing field value, (3) an incorrect UTI, (4) a security-based swap that is not reported, (5) a security-based swap that is closed that should be open, (6) a security-based swap that is open that should be closed, (7) a security-based swap that is reported that should not have been reported, or (8) a security-based swap who’s counterparty’s identifier should be updated; then the Client is required to resubmit and correct the UTI(s). After submitting all of the corrections, the Client should re-execute the open security-based swaps verification report and verify the identified security-based swaps are now correct. This process shall not be re-executed after each individual security-based swap is corrected, but instead after the Client believes all incorrect security-based swaps have been corrected. This process should be repeated until the Client has verified that the open security-based swaps report is in line with their internal books and records.

8.3.2 Delegated Reporters and Authorized Access Clients

Where a Reporting Client has notified the KOR SBSDR and systematically granted access to a Delegated Reporter or Authorized Access Client, the Delegated Reporter or Authorized Access Client will be provided with the same data access as Reporting Side. The access for the Delegated Reporter or Authorized Access Client shall be in addition to the access for the Reporting Side. The Client is responsible for granting and revoking access to the Delegated Reporter or Authorized Access Client when appropriate.

Reference the User Guide for instructions detailing how each Client can grant and revoke access regarding a Delegated Reporter or Authorized Access Client.

9.0 KOR SBSDR duties and obligations regarding securities based swaps reporting

9.1 Time stamping incoming information

A registered security-based swap data repository shall time stamp, to the second, its receipt of any information submitted to it pursuant to SEC Rule(s) § 242.901 (c), (d), (e), or (i).

References: SEC Rule(s) § 242.901(f).

9.2 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.

References: SEC Rule 240.13n-5(b)(5)

9.3 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.

References: SEC Rule(s) § 242.905(b), 242.905(b)(1), and 242.905(b)(2).

9.4 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.

References SEC Rule 240.13n-5(b)(4), 240.13n-5(b)(4)(i), and 240.13n-5(b)(4)(ii).

9.5 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. These aggregated views are available by Reporting Side LEI using one or more of the following attributes:

a. Asset Class

b. UPI

c. Underlying instrument

d. Counterparty

References: SEC Rule 240.13n-5(b)(2).

10.0 Publicly disseminated security-based swaps^29

Publicly disseminated security-based swaps^29: Public Dissemination as of Compliance Date 2 (currently February 14, 2022)

10.1 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^30. 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^31 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).

closed^30: 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]

flags^31: 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.

10.2 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.

Reference Public Website Guide.

10.3 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.

10.4 Non-disseminated information

A registered security-based swap data repository shall 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.

Reference SEC Rule(s) § 242.901, 242.902(c), 242.902(c)(1), 242.902(c)(2), 242.902(c)(3), 242.902(c)(4), 242.902(c)(5), 242.902(c)(6), 242.902(c)(7), 242.902(c)(8), 242.908(a)(1), and 242.908(a)(2).

10.5 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.

References SEC Rule(s) § 242.902(d).

10.6 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.

10.6.1 Notional rounding and capping

KOR SBSDR has implemented rounding practices consistent with CFTC Rules 43.4(f)-(h)^37

KOR SBSDR has implemented capping practices consistent with CFTC Rules 43.4(f)-(h) with the exception 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, where KOR will disseminate a capped size of $5 million (e.g., “$5MM+” or similar) in lieu of the true notional size.

In order for KOR to accurately cap publicly disseminated trades, those not executed in USD must be provided in a USD equivalent notional amount. Clients may use a currency exchange rate that is widely published within the preceding two Business Days from the date of execution of the swap transaction.

References: CFTC Rule(s) §43.4(e).
References SEC Cross-Border Release

CFTC Rules 43.4(f)-(h)^37 : 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

11.0 Dispute Resolution

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 KOR 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 are 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.

References: SEC rule 240.13n-5(b)(6)

12.0 Chief Compliance Officer

12.1 CCO Designation

KOR SBSDR will at all times have a Chief Compliance Officer. KOR shall identify on Form SBSDR (17 CFR 249.1500) a person who has been designated by the board to serve as a chief compliance officer of the security-based swap data repository. The compensation, appointment, and removal of the chief compliance officer shall require the approval of a majority of the security-based swap data repository's board.

Reference SEC Rule 240.13n-11(a) and 240.13n-4(b)(11).

12.2 CCO Supervision

The CCO shall be provided adequate authority and resources to develop and enforce the policies and procedures developed to ensure compliance and fulfill the duties set forth in this Rulebook. The CCO is responsible for overseeing the KOR SBSDR Compliance Department and ensuring compliance with the Rules as applicable. On a periodic basis and as needed, the CCO shall consult with the CEO on the adequacy of resources and make recommendations where needed.

The CCO has supervisory authority to inspect books and records and interview KOR SBSDR employees. Upon identification of a potential violation of any regulatory requirement or internal policy or procedure, the CCO is responsible for taking steps to investigate and remediate any such matter.

12.3 CCO Qualifications

The CCO shall have the “background and skills appropriate for fulfilling the responsibilities of the position.” KOR senior management has identified the minimum standards that must be met for an individual to be considered to have the background and skills necessary to carry out the duties of the position of CCO. Below is a list of the qualifications identified and considered when the candidate for the position of CCO is recommended to the BOD for approval and appointment:

a. The individual may not be subject to any conviction or injunction of a type described in Sections 15(b)(4)(B) or (C) of the Exchange Act within the past ten years.

b. The individual may not be subject to any action of a self-regulatory organization with respect to such person imposing a final disciplinary sanction pursuant to Sections 6(b)(6), l5A(b)(7), or 17A(b)(3)(G) of the Exchange Act.

c. The individual may not be subject to any final action by a self-regulatory organization with respect to such person constituting a denial, bar, prohibition, or limitation of membership, participation, or association with a member, or of access to services offered by such organization or a member thereof.

d. The individual may not be subject to any final action by another federal regulatory agency, including the Securities and Exchange Commission, Commodity Futures Trading Commission, any state regulatory agency, or any foreign financial regulatory authority resulting in:

    i. a finding that such person has made a false statement or omission, or has been dishonest, unfair, or unethical;

    ii. a finding that such person has been involved in a violation of any securities-related regulations or statutes;

    iii. a finding that such person has been a cause of a business having its authorization to do business denied, suspended, revoked, or restricted;

    iv. an order entered, in the past ten years, against such person in connection with a securities-related activity; or

    v. any disciplinary sanction, including a denial, suspension, or revocation of such person's registration or license or otherwise, by order, a prevention from associating with a securities-related business or a restriction of such person's activities.

e. The individual must have sufficient compliance experience to carry out its responsibilities. Such experience could be demonstrated by:

i. Previously holding the title of CCO, as long as the firm at which the individual held such title has not been designated as a disciplined firm subject to enhanced supervisory requirements imposed by NFA or FINRA.

ii. Functioned in a compliance role or compliance supporting function for a minimum of seven years.

iii. The individual possesses product knowledge sufficient to make any such decision required of the CCO.

13.0 KOR SBSDR system

13.1 Hours of Operation

The KOR SBSDR operates 7 days per week, 24 hours per day; including the KOR SBSDR User Interface and the KOR SBSDR Public Website. KOR SBSDR does not have planned system downtime to perform system maintenance or updates. In the event of scheduled maintenance that requires special closing hours, those hours will be the least disruptive to the KOR SBSDR's reporting responsibilities. KOR SBSDR will provide reasonable advanced notice to Clients and the public. During any ad hoc scheduled or unplanned system closures, KOR SBSDR will accept and hold in queue SBSDR Data submitted by Clients and shall promptly process all SBSDR Data received during the closure. If an unplanned outage causes the KOR SBSDR to be unable to receive and hold SBSDR Data in a queue, then KOR SBSDR will promptly notify Clients and the public of the outage and will again notify them immediately upon resumption of normal operations.

References: SEC Rule(s) §242.904, 242.904(a), 242.904(b), 242.904(c), 242.904(d), and 242.904(e).

13.2 Emergency policies and procedures

KOR has developed a comprehensive Business Continuity and Disaster Recovery Program. The KOR SBSDR is included within the broader Business Continuity and Disaster Recovery Program applicable to KOR as a whole. These policies shall enumerate the circumstances under which the KOR SBSDR is authorized to invoke its Emergency authority and the procedures that it shall follow to declare an Emergency. Such policies and procedures shall also address the range of measures that it is authorized to take when exercising such Emergency authority.

The Board of Directors have the power to act in emergencies. In the event that the BOD determines than an emergency situation exists in which the operation of the KOR SBSDR is likely to be disrupted, the integrity of the data maintained by the KOR SBSDR threatened, or the normal functioning of the KOR SBSDR has been or is likely to be disrupted, or a KOR SBSDR

Significant Action occurs, the board may, upon a majority vote of the members present or upon a majority vote of the members who respond to a poll, take such action as may in the Board's sole discretion appear necessary to prevent, correct or alleviate the emergency condition. In responding to an emergency situation, the directors who abstain from voting on a Significant Action shall not be counted in determining whether such action was approved by a majority vote, but such members can be counted for the purpose of determining whether a quorum exists. Without limiting the foregoing, the board may (1) stop accepting derivatives data, (2) suspend direct electronic access to the KOR SBSDR (3) suspected real-time reporting of derivatives data and (4) modify the operating days or hours.

In the event a Client or User affected by the Emergency action, the KOR SBSDR shall contact the Client or User as soon as reasonably practicable after taking any action.

13.3 Systems Safeguards

13.3.1 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.

13.3.2 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.

13.4 Fees to use KOR SBSDR services

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.

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

References SEC Rules 240.13n-4(c)(1)(i).

14.0 Disciplinary procedures

14.1 Violation of KOR SBSDR rules

The CCO or his or her designee is responsible for investigation of any potential violation of the KOR SBSDR Rulebook. The CCO has the authority to request information of any Client as part of an investigation of any rule violation. Rule violations will be documented, and all supporting documentation will be retained. If deemed necessary by the CCO, a Client or User’s access may be suspended or revoked. The CCO is also responsible for making a decision to restore a Client or User’s access by conducting a comprehensive review of a Client’s compliance with regulatory requirements as well as KOR SBSDR Rules, as applicable.

14.2 Client Denial, Revocation, or Suspension

KOR Reporting has the right to decline, revoke, or suspend a Client. Market Participants may be denied access pursuant to Applicable Law (e.g., OFAC or the direction of a regulator), violation of KOR SBSDR Rules, or improper use of the system. KOR shall notify the applicable regulator of any Client whose access has been denied, revoked, or suspended due to Applicable Law. Final determination to decline, revoke, or suspend a Client shall be made by the Chief Compliance Officer.

In the event a Client is denied, revoked, or suspended; KOR shall provide the Market Participant written notice containing the grounds for determination and the opportunity to appeal the decision to the CCO and Board of Directors by written request.

14.3 Restoring Client Access

KOR may restore access to a Client after approval from the CCO and/or the Board of Directors. The CCO shall take under consideration Applicable Law, regulatory requirements, and the Market Participant’s response to the cause of denial, revocation, or suspension. All decisions shall be documented when determining whether to restore access.