

price (if applicable); size (displayed and non-displayed); side (buy/sell); order type; if a sell order, whether the order is long, short, short exempt; open/close indicator; time in force (if applicable); if the order is for a listed option, option type (put/call), option symbol or root symbol, underlying symbol, strike price, expiration date, and open/close; and any special handling instructions.

(8) The term *order* shall include:

(i) Any order received by a member of a national securities exchange or national securities association from any person;

(ii) Any order originated by a member of a national securities exchange or national securities association; or

(iii) Any bid or offer.

(9) The term *reportable event* shall include, but not be limited to, the original receipt or origination, modification, cancellation, routing, and execution (in whole or in part) of an order, and receipt of a routed order.

[77 FR 45808, Aug. 1, 2012]

§ 242.614 Registration and responsibilities of competing consolidators.

(a) *Competing consolidator registration*—(1) *Initial Form CC*—(i) *Filing and effectiveness requirement*. No person, other than a national securities exchange or a national securities association:

(A) May receive directly, pursuant to an effective national market system plan, from a national securities exchange or national securities association information with respect to quotations for and transactions in NMS stocks; and

(B) Generate a consolidated market data product for dissemination to any person unless the person files with the Commission an initial Form CC and the initial Form CC has become effective pursuant to paragraph (a)(1)(v) of this section.

(ii) *Electronic filing and submission*. Any reports to the Commission required under this section shall be filed electronically on Form CC (17 CFR 249.1002), include all information as prescribed in Form CC and the instructions thereto, and contain an electronic signature as defined in § 240.19b-4(j) of this chapter.

(iii) *Commission review period*. The Commission may, by order, as provided in paragraph (a)(1)(v)(B) of this section, declare an initial Form CC filed by a competing consolidator ineffective no later than 90 calendar days from the date of filing with the Commission.

(iv) *Withdrawal of initial Form CC due to inaccurate or incomplete disclosures*. During the review by the Commission of the initial Form CC, if any information disclosed in the initial Form CC is or becomes inaccurate or incomplete, the competing consolidator shall promptly withdraw the initial Form CC and may refile an initial Form CC pursuant to paragraph (a)(1) of this section.

(v) *Effectiveness; ineffectiveness determination*. (A) An initial Form CC filed by a competing consolidator will become effective, unless declared ineffective, no later than the expiration of the review period provided in paragraph (a)(1)(iii) of this section and publication pursuant to paragraph (b)(2)(i) of this section.

(B) The Commission shall, by order, declare an initial Form CC ineffective if it finds, after notice and opportunity for hearing, that such action is necessary or appropriate in the public interest, and is consistent with the protection of investors. If the Commission declares an initial Form CC ineffective, the competing consolidator shall be prohibited from operating as a competing consolidator. An initial Form CC declared ineffective does not prevent the competing consolidator from subsequently filing a new Form CC.

(2) *Form CC amendments*. A competing consolidator shall amend a Form CC:

(i) Prior to the implementation of a material change to the pricing, connectivity, or products offered (“material amendment”); and

(ii) No later than 30 calendar days after the end of each calendar year to correct information that has become inaccurate or incomplete for any reason and to provide an Annual Report as required under Form CC (each a “Form CC amendment”).

(3) *Notice of cessation*. A competing consolidator shall notice its cessation of operations on Form CC at least 90 calendar days prior to the date the competing consolidator will cease to

operate as a competing consolidator. The notice of cessation shall cause the Form CC to become ineffective on the date designated by the competing consolidator.

(4) *Date of filing.* For purposes of filings made pursuant to this section:

(i) The term *business day* shall have the same meaning as defined in § 240.19b–4(b)(2) of this chapter.

(ii) If the conditions of this section and Form CC are otherwise satisfied, all filings submitted electronically on or before 5:30 p.m. Eastern Standard Time or Eastern Daylight Saving Time, whichever is currently in effect, on a business day, shall be deemed filed on that business day, and all filings submitted after 5:30 p.m. Eastern Standard Time or Eastern Daylight Saving Time, whichever is currently in effect, shall be deemed filed on the next business day.

(b) *Public disclosures.* (1) Every Form CC filed pursuant to this section shall constitute a “report” within the meaning of sections 11A, 17(a), 18(a), and 32(a) of the Act (15 U.S.C. 78k–1, 78q(a), 78r(a), and 78ff(a)), and any other applicable provisions of the Act.

(2) The Commission will make public via posting on the Commission’s website:

(i) Identification of each competing consolidator that has filed an initial Form CC with the Commission and the date of filing;

(ii) Each effective initial Form CC, as amended;

(iii) Each order of ineffective initial Form CC;

(iv) Each Form CC amendment. The Commission will make public the entirety of any Form CC amendment no later than 30 calendar days from the date of filing thereof with the Commission; and

(v) Each notice of cessation.

(c) *Posting of hyperlink to the Commission’s website.* Each competing consolidator shall make public via posting on its website a direct URL hyperlink to the Commission’s website that contains the documents enumerated in paragraphs (b)(2)(i) through (v) of this section.

(d) *Responsibilities of competing consolidators.* Each competing consolidator shall:

(1) Collect from each national securities exchange and national securities association, either directly or indirectly, any information with respect to quotations for and transactions in NMS stocks as provided in § 242.603(b) that is necessary to create a consolidated market data product, as defined in § 242.600(b)(20).

(2) Calculate and generate a consolidated market data product, as defined in § 242.600(b)(20), from the information collected pursuant to paragraph (d)(1) of this section.

(3) Make a consolidated market data product, as defined in § 242.600(b)(20), as timestamped as required by paragraph (d)(4) of this section and including the national securities exchange and national securities association data generation timestamp required to be provided by the national securities exchange and national securities association participants by paragraph (e)(2) of this section, available to subscribers on a consolidated basis on terms that are not unreasonably discriminatory.

(4) Timestamp the information collected pursuant to paragraph (d)(1) of this section upon:

(i) Receipt from each national securities exchange and national securities association;

(ii) Receipt of such information at its aggregation mechanism; and

(iii) Dissemination of a consolidated market data product to subscribers.

(5) Within 15 calendar days after the end of each month, publish prominently on its website monthly performance metrics, as defined by the effective national market system plan(s) for NMS stocks, that shall include at least the information in paragraphs (d)(5)(i) through (v) of this section. All information must be publicly posted in downloadable files and must remain free and accessible (without any encumbrances or restrictions) by the general public on the website for a period of not less than three years from the initial date of posting.

(i) Capacity statistics;

(ii) Message rate and total statistics;

(iii) System availability;

(iv) Network delay statistics; and

(v) Latency statistics for the following, with distribution statistics up to the 99.99th percentile:

Securities and Exchange Commission

§ 242.614

(A) When a national securities exchange or national securities association sends an inbound message to a competing consolidator network and when the competing consolidator network receives the inbound message;

(B) When the competing consolidator network receives the inbound message and when the competing consolidator network sends the corresponding consolidated message to a subscriber; and

(C) When a national securities exchange or national securities association sends an inbound message to a competing consolidator network and when the competing consolidator network sends the corresponding consolidated message to a subscriber.

(6) Within 15 calendar days after the end of each month, publish prominently on its website the information in paragraphs (d)(6)(i) through (v) of this section. All information must be publicly posted and must remain free and accessible (without any encumbrances or restrictions) by the general public on the website for a period of not less than three years from the initial date of posting.

(i) Data quality issues;

(ii) System issues;

(iii) Any clock synchronization protocol utilized;

(iv) For the clocks used to generate the timestamps described in paragraph (d)(4) of this section, the clock drift averages and peaks, and the number of instances of clock drift greater than 100 microseconds; and

(v) Vendor alerts.

(7) Keep and preserve at least one copy of all documents, including all correspondence, memoranda, papers, books, notices, accounts, and such other records as shall be made or received by it in the course of its business as such and in the conduct of its business. Competing consolidators shall keep all such documents for a period of no less than five years, the first two years in an easily accessible place.

(8) Upon request of any representative of the Commission, promptly furnish to the possession of such representative copies of any documents required to be kept and preserved by it.

(9) Each competing consolidator that is not required to comply with the requirements of §§ 242.1000 through

242.1007 regarding systems compliance and integrity (Regulation SCI) shall comply with the following:

(i) *Definitions.* For purposes of this paragraph (d)(9), the following definitions shall apply:

Systems disruption means an event in a competing consolidator's systems involved in the collection and consolidation of consolidated market data, and dissemination of consolidated market data products, that disrupts, or significantly degrades, the normal operation of such systems.

Systems intrusion means any unauthorized entry into a competing consolidator's systems involved in the collection and consolidation of consolidated market data, and dissemination of consolidated market data products.

(ii) *Obligations relating to policies and procedures.* (A)(1) Establish, maintain, and enforce written policies and procedures reasonably designed to ensure: That its systems involved in the collection and consolidation of consolidated market data, and dissemination of consolidated market data products have levels of capacity, integrity, resiliency, availability, and security adequate to maintain the competing consolidator's operational capability and promote the maintenance of fair and orderly markets; and the prompt, accurate, and reliable dissemination of consolidated market data products.

(2) Such policies and procedures shall be deemed to be reasonably designed if they are consistent with current industry standards, which shall be comprised of information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization. Compliance with such current industry standards, however, shall not be the exclusive means to comply with the requirements of this paragraph (d)(9)(ii)(A);

(B) Periodically review the effectiveness of the policies and procedures required by paragraph (d)(9)(ii)(A) of this section, and take prompt action to remedy deficiencies in such policies and procedures; and

(C) Establish, maintain, and enforce reasonably designed written policies and procedures that include the criteria for identifying responsible personnel, the designation and documentation of responsible personnel, and escalation procedures to quickly inform responsible personnel of potential systems disruptions and systems intrusions; and periodically review the effectiveness of the policies and procedures, and take prompt action to remedy deficiencies.

(iii) *Systems disruptions or systems intrusions.* (A) Upon responsible personnel having a reasonable basis to conclude that a systems disruption or systems intrusion has occurred, begin to take appropriate corrective action which shall include, at a minimum, mitigating potential harm to investors and market integrity resulting from the event and devoting adequate resources to remedy the event as soon as reasonably practicable.

(B) Promptly upon responsible personnel having a reasonable basis to conclude that a systems disruption (other than a system disruption that has had, or the competing consolidator reasonably estimates would have, no or a de minimis impact on the competing consolidator's operations or on market participants) has occurred, publicly disseminate information relating to the event (including the system(s) affected and a summary description); when known, promptly publicly disseminate additional information relating to the event (including a detailed description, an assessment of those potentially affected, a description of the progress of corrective action and when the event has been or is expected to be resolved); and until resolved, provide regular updates with respect to such information.

(C) Concurrent with public dissemination of information relating to a systems disruption pursuant to paragraph (d)(9)(iii)(B) of this section, or promptly upon responsible personnel having a reasonable basis to conclude that a systems intrusion (other than a system intrusion that has had, or the competing consolidator reasonably estimates would have, no or a de minimis impact on the competing consolidator's operations or on market participants) has

occurred, provide the Commission notification and, until resolved, updates of such event. Notifications required pursuant to this paragraph (d)(9)(iii)(C) shall include information relating to the event (including the system(s) affected and a summary description); when known, additional information relating to the event (including a detailed description, an assessment of those potentially affected, a description of the progress of corrective action and when the event has been or is expected to be resolved); and until resolved, regular updates with respect to such information. Notifications relating to systems disruptions and systems intrusions pursuant to this paragraph (d)(9)(iii)(C) shall be submitted to the Commission on Form CC.

(iv) *Coordinated testing.* Participate in the industry- or sector-wide coordinated testing of business recovery and disaster recovery plans required of SCI entities pursuant to § 242.1004(c).

(e) *Amendment of the effective national market system plan(s) for NMS stocks.* The participants to the effective national market system plan(s) for NMS stocks shall file with the Commission, pursuant to § 242.608, an amendment that includes the following provisions within 150 calendar days from June 8, 2021:

(1) Conforming the effective national market system plan(s) for NMS stocks to reflect provision of information with respect to quotations for and transactions in NMS stocks that is necessary to generate consolidated market data by the national securities exchange and national securities association participants to competing consolidators and self-aggregators;

(2) The application of timestamps by the national securities exchange and national securities association participants on all information with respect to quotations for and transactions in NMS stocks that is necessary to generate consolidated market data, including the time that such information was generated as applicable by the national securities exchange or national securities association and the time the national securities exchange or national securities association made such information available to competing consolidators and self-aggregators;

Securities and Exchange Commission

§ 242.900

(3) Assessments of competing consolidator performance, including speed, reliability, and cost of data provision and the provision of an annual report of such assessment to the Commission, and the Commission will make the annual report publicly available on the Commission's website;

(4) The development, maintenance, and publication of a list that identifies the primary listing exchange for each NMS stock; and

(5) The calculation and publication on a monthly basis of consolidated market data gross revenues for NMS stocks as specified by:

(i) Listed on the New York Stock Exchange (NYSE);

(ii) Listed on Nasdaq; and

(iii) Listed on exchanges other than NYSE or Nasdaq.

[86 FR 18811, Apr. 9, 2021]

REGULATION SBSR—REGULATORY REPORTING AND PUBLIC DISSEMINATION OF SECURITY-BASED SWAP INFORMATION

SOURCE: 80 FR 14728, Mar. 19, 2015, unless otherwise noted.

§ 242.900 Definitions.

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:

(a) *Affiliate* means any person that, directly or indirectly, controls, is controlled by, or is under common control with, a person.

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

(c) [Reserved].

(d) *Branch ID* means the UIC assigned to a branch or other unincorporated office of a participant.

(e) *Broker ID* means the UIC assigned to a person acting as a broker for a participant.

(f) *Business day* means a day, based on U.S. Eastern Time, other than a

Saturday, Sunday, or a U.S. federal holiday.

(g) *Clearing transaction* means a security-based swap that has a registered clearing agency as a direct counterparty.

(h) *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:

(1) Is a director, general partner or officer exercising executive responsibility (or having similar status or functions);

(2) 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

(3) In the case of a partnership, has the right to receive, upon dissolution, or has contributed, 25 percent or more of the capital.

(i) *Counterparty* means a person that is a direct counterparty or indirect counterparty of a security-based swap.

(j) *Counterparty ID* means the UIC assigned to a counterparty to a security-based swap.

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

(l) *Direct electronic access* has the same meaning as in § 240.13n-4(a)(5) of this chapter.

(m) *Exchange Act* means the Securities Exchange Act of 1934 (15 U.S.C. 78a *et seq.*), as amended.

(n) *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.

(o) *Foreign branch* has the same meaning as in § 240.3a71-3(a)(1) of this chapter.

(p) *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.

(q) *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.

(r) *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.

(s) *Non-U.S. person* means a person that is not a U.S. person.

(t) *Parent* means a legal person that controls a participant.

(u) *Participant*, with respect to a registered security-based swap data repository, means:

(1) 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);

(2) A platform that reports a security-based swap to that registered security-based swap data repository to satisfy an obligation under § 242.901(a);

(3) 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

(4) 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).

(v) *Platform* means a national securities exchange or security-based swap execution facility that is registered or exempt from registration.

(w) *Platform ID* means the UIC assigned to a platform on which a security-based swap is executed.

(x) *Post-trade processor* means any person that provides affirmation, confirmation, matching, reporting, or clearing services for a security-based swap transaction.

(y) *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.

(z) *Price* means the price of a security-based swap transaction, expressed in terms of the commercial conventions used in that asset class.

(aa) *Product* means a group of security-based swap contracts each having the same material economic terms except those relating to price and size.

(bb) *Product ID* means the UIC assigned to a product.

(cc) *Publicly disseminate* means to make available through the Internet or other electronic data feed that is widely accessible and in machine-readable electronic format.

(dd) [Reserved].

(ee) *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.

Securities and Exchange Commission

§ 242.901

(ff) *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.

(gg) *Reporting side* means the side of a security-based swap identified by § 242.901(a)(2).

(hh) *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.

(ii) *Time of execution* means the point at which the counterparties to a security-based swap become irrevocably bound under applicable law.

(jj) *Trader ID* means the UIC assigned to a natural person who executes one or more security-based swaps on behalf of a direct counterparty.

(kk) *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.

(ll) *Trading desk ID* means the UIC assigned to the trading desk of a participant.

(mm) *Transaction ID* means the UIC assigned to a specific security-based swap transaction.

(nn) *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.

(oo) *Ultimate parent* means a legal person that controls a participant and that itself has no parent.

(pp) *Ultimate parent ID* means the UIC assigned to an ultimate parent of a participant.

(qq) *Unique Identification Code or UIC* means a unique identification code assigned to a person, unit of a person, product, or transaction.

(rr) *United States* has the same meaning as in § 240.3a71-3(a)(5) of this chapter.

(ss) *U.S. person* has the same meaning as in § 240.3a71-3(a)(4) of this chapter.

(tt) *Widely accessible*, as used in paragraph (cc) of this section, means widely available to users of the information on a non-fee basis.

[80 FR 14728, Mar. 19, 2015, as amended at 81 FR 53653, Aug. 12, 2016]

§ 242.901 Reporting obligations.

(a) *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:

(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 paragraph (c) of this section (except that, with respect to paragraph (c)(5) of this section, the platform need indicate only if both direct counterparties are registered security-based swap dealers) and paragraphs (d)(9) and (10) of this section.

(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 §§ 242.900 through 242.909 to a registered security-based swap data repository. The reporting side shall be determined as follows:

(i) *Clearing transactions.* For a clearing transaction, the reporting side is the registered clearing agency that is a counterparty to the transaction.

(ii) *Security-based swaps other than clearing transactions.* (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:

(1) If both sides include a U.S. person, the sides shall select the reporting side.

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

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

(4) If neither side includes a U.S. person and neither side includes a non-U.S. person that falls within § 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 paragraph (c) of this section (except that, with respect to paragraph (c)(5) of this section, 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 paragraphs (d)(9) and (10) of this section.

(3) *Notification to registered clearing agency.* A person who, under paragraph (a)(1) or (a)(2)(ii) of this section, 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 clear-

ing 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.

(b) *Alternate recipient of security-based swap information.* If there is no registered security-based swap data repository that will accept the report required by § 242.901(a), the person required to make such report shall instead provide the required information to the Commission.

(c) *Primary trade information.* The reporting side shall report the following information within the timeframe specified in paragraph (j) of this section:

(1) The product ID, if available. If the security-based swap has no product ID, or if the product ID does not include the following information, the reporting side shall report:

(i) Information that identifies the security-based swap, including the asset class of the security-based swap and the specific underlying reference asset(s), reference issuer(s), or reference index;

(ii) The effective date;

(iii) The scheduled termination date;

(iv) The terms of any standardized fixed or floating rate payments, and the frequency of any such payments; and

(v) If the security-based swap is customized to the extent that the information provided in paragraphs (c)(1)(i) through (iv) of this section does not provide all of the material information necessary to identify such customized security-based swap or does not contain the data elements necessary to calculate the price, a flag to that effect;

(2) The date and time, to the second, of execution, expressed using Coordinated Universal Time (UTC);

(3) The price, including the currency in which the price is expressed and the amount(s) and currenc(ies) of any upfront payments;

(4) The notional amount(s) and the currenc(ies) in which the notional amount(s) is expressed;

(5) If both sides of the security-based swap include a registered security-

Securities and Exchange Commission

§ 242.901

based swap dealer, an indication to that effect;

(6) Whether the direct counterparties intend that the security-based swap will be submitted to clearing; and

(7) If applicable, any flags pertaining to the transaction that are specified in the policies and procedures of the registered security-based swap data repository to which the transaction will be reported.

(d) *Secondary trade information.* In addition to the information required under paragraph (c) of this section, for each security-based swap for which it is the reporting side, the reporting side shall report the following information within the timeframe specified in paragraph (j) of this section:

(1) The counterparty ID or the execution agent ID of each counterparty, as applicable;

(2) As applicable, the branch ID, broker ID, execution agent ID, trader ID, and trading desk ID of the direct counterparty on the reporting side;

(3) To the extent not provided pursuant to paragraph (c)(1) of this section, the terms of any fixed or floating rate payments, or otherwise customized or non-standard payment streams, including the frequency and contingencies of any such payments;

(4) For a security-based swap that is not a clearing transaction and that will not be allocated after execution, the title and date of any master agreement, collateral agreement, margin agreement, or any other agreement incorporated by reference into the security-based swap contract;

(5) To the extent not provided pursuant to paragraph (c) of this section or other provisions of this paragraph (d), any additional data elements included in the agreement between the counterparties that are necessary for a person to determine the market value of the transaction;

(6) If applicable, and to the extent not provided pursuant to paragraph (c) of this section, the name of the clearing agency to which the security-based swap will be submitted for clearing;

(7) If the direct counterparties do not intend to submit the security-based swap to clearing, whether they have invoked the exception in Section 3C(g) of the Exchange Act (15 U.S.C. 78c-3(g));

(8) To the extent not provided pursuant to the other provisions of this paragraph (d), if the direct counterparties do not submit the security-based swap to clearing, a description of the settlement terms, including whether the security-based swap is cash-settled or physically settled, and the method for determining the settlement value;

(9) The platform ID, if applicable, or if a registered broker-dealer (including a registered security-based swap execution facility) is required to report the security-based swap by § 242.901(a)(2)(ii)(E)(4), the broker ID of that registered broker-dealer (including a registered security-based swap execution facility); and

(10) If the security-based swap arises from the allocation, termination, novation, or assignment of one or more existing security-based swaps, the transaction ID of the allocated, terminated, assigned, or novated security-based swap(s), except in the case of a clearing transaction that results from the netting or compression of other clearing transactions.

(e) *Reporting of life cycle events.* (1)(i) *Generally.* A life cycle event, and any adjustment due to a life cycle event, that results in a change to information previously reported pursuant to paragraph (c), (d), or (i) of this section 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.

(ii) *Acceptance for clearing.* A registered clearing agency shall report whether or not it has accepted a security-based swap for clearing.

(2) All reports of life cycle events and adjustments due to life cycle events shall, within the timeframe specified in paragraph (j) of this section, 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.

(f) *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 paragraph (c), (d), (e), or (i) of this section.

(g) *Assigning transaction ID.* A registered security-based swap data repository shall assign a transaction ID to each security-based swap, or establish or endorse a methodology for transaction IDs to be assigned by third parties.

(h) *Format of reported information.* A person having a duty to report shall electronically transmit the information required under this section in a format required by the registered security-based swap data repository to which it reports.

(i) *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 paragraphs (c) and (d) of this section 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.

(j) *Interim timeframe for reporting.* The reporting timeframe for paragraphs (c) and (d) of this section 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. The reporting timeframe for paragraph (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.

APPENDIX TO 17 CFR 242.901 REPORTS REGARDING THE ESTABLISHMENT OF BLOCK THRESHOLDS AND REPORTING DELAYS FOR REGULATORY REPORTING OF SECURITY-BASED SWAP TRANSACTION DATA

This appendix sets forth guidelines applicable to reports that the Commission has directed its staff to make in connection with the determination of block thresholds and reporting delays for security-based swap transaction data. The Commission intends to use these reports to inform its specification of the criteria for determining what con-

stitutes a large notional security-based swap transaction (block trade) for particular markets and contracts; and the appropriate time delay for reporting large notional security-based swap transactions (block trades) to the public in order to implement regulatory requirements under Section 13 of the Act (15 U.S.C. 78m). In producing these reports, the staff shall consider security-based swap data collected by the Commission pursuant to other Title VII rules, as well as any other applicable information as the staff may determine to be appropriate for its analysis.

(a) *Report topics.* As appropriate, based on the availability of data and information, the reports should address the following topics for each asset class:

(1) *Price impact.* In connection with the Commission's obligation to specify criteria for determining what constitutes a block trade and the appropriate reporting delay for block trades, the report generally should assess the effect of notional amount and observed reporting delay on price impact of trades in the security-based swap market.

(2) *Hedging.* In connection with the Commission's obligation to specify criteria for determining what constitutes a block trade and the appropriate reporting delay for block trades, the report generally should consider potential relationships between observed reporting delays and the incidence and cost of hedging large trades in the security-based swap market, and whether these relationships differ for interdealer trades and dealer to customer trades.

(3) *Price efficiency.* In connection with the Commission's obligation to specify criteria for determining what constitutes a block trade and the appropriate reporting delay for block trades, the report generally should assess the relationship between reporting delays and the speed with which transaction information is impounded into market prices, estimating this relationship for trades of different notional amounts.

(4) *Other topics.* Any other analysis of security-based swap data and information, such as security-based swap market liquidity and price volatility, that the Commission or the staff deem relevant to the specification of:

(i) The criteria for determining what constitutes a large notional security-based swap transaction (block trade) for particular markets and contracts; and

(ii) The appropriate time delay for reporting large notional security-based swap transactions (block trades).

(b) *Timing of reports.* Each report shall be complete no later than two years following the initiation of public dissemination of security-based swap transaction data by the first registered SDR in that asset class.

(c) *Public comment on the report.* Following completion of the report, the report shall be

Securities and Exchange Commission

§ 242.903

published in the FEDERAL REGISTER for public comment.

[80 FR 14728, Mar. 19, 2015, as amended at 81 FR 53653, Aug. 12, 2016]

§ 242.902 Public dissemination of transaction reports.

(a) *General.* Except as provided in paragraph (c) of this section, a registered security-based swap data repository shall publicly disseminate a transaction report of a security-based swap, or a life cycle event or adjustment due to a life cycle event, immediately upon receipt of information about the security-based swap, or upon re-opening following a period when the registered security-based swap data repository was closed. The transaction report shall consist of all the information reported pursuant to § 242.901(c), plus any condition flags contemplated by the registered security-based swap data repository's policies and procedures that are required by § 242.907.

(b) [Reserved].

(c) *Non-disseminated information.* A registered security-based swap data repository shall not disseminate:

(1) The identity of any counterparty to a security-based swap;

(2) 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;

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

(4) Any non-mandatory report;

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

(6) 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;

(7) Any information regarding the allocation of a security-based swap; or

(8) 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.

(d) *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.

[80 FR 14728, Mar. 19, 2015, as amended at 81 FR 53654, Aug. 12, 2016]

§ 242.903 Coded information.

(a) If an internationally recognized standards-setting system that imposes fees and usage restrictions on persons that obtain UICs for their own usage that are fair and reasonable and not unreasonably discriminatory and that meets the criteria of paragraph (b) of this section is recognized by the Commission and has assigned a UIC to a person, unit of a person, or product (or has endorsed a methodology for assigning transaction IDs), the registered security-based swap data repository shall employ that UIC (or methodology for assigning transaction IDs). If no such system has been recognized by the Commission, or a recognized system has not assigned a UIC to a particular person, unit of a person, or product (or has not endorsed a methodology for assigning transaction IDs), the registered security-based swap data repository shall assign a UIC to that person, unit of person, or product using its own methodology (or endorse a methodology for assigning transaction IDs). If the Commission has recognized such a system that assigns UICs to persons, each participant of a registered security-based swap data repository shall obtain a UIC from or through that system for identifying itself, and each participant that acts as a guarantor of a direct counterparty's performance of any obligation under a security-based swap that is subject to § 242.908(a) shall, if the direct counterparty has not already done so, obtain a UIC for identifying the direct counterparty from or through that system, if that system

§ 242.904

permits third-party registration without a requirement to obtain prior permission of the direct counterparty.

(b) A registered security-based swap data repository may permit information to be reported pursuant to § 242.901, and may publicly disseminate that information pursuant to § 242.902, using codes in place of certain data elements, provided that the information necessary to interpret such codes is widely available to users of the information on a non-fee basis.

§ 242.904 Operating hours of registered security-based swap data repositories.

A registered security-based swap data repository shall have systems in place to continuously receive and disseminate information regarding security-based swaps pursuant to §§ 242.900 through 242.909, subject to the following exceptions:

(a) A registered security-based swap data repository may establish normal closing hours during periods when, in its estimation, the U.S. market and major foreign markets are inactive. A registered security-based swap data repository shall provide reasonable advance notice to participants and to the public of its normal closing hours.

(b) A registered security-based swap data repository may declare, on an *ad hoc* basis, special closing hours to perform system maintenance that cannot wait until normal closing hours. A registered security-based swap data repository shall, to the extent reasonably possible under the circumstances, avoid scheduling special closing hours during periods when, in its estimation, the U.S. market and major foreign markets are most active; and provide reasonable advance notice of its special closing hours to participants and to the public.

(c) During normal closing hours, and to the extent reasonably practicable during special closing hours, a registered security-based swap data repository shall have the capability to receive and hold in queue information regarding security-based swaps that has been reported pursuant to §§ 242.900 through 242.909.

(d) When a registered security-based swap data repository re-opens fol-

lowing normal closing hours or special closing hours, it shall disseminate transaction reports of security-based swaps held in queue, in accordance with the requirements of § 242.902.

(e) If a registered security-based swap data repository could not receive and hold in queue transaction information that was required to be reported pursuant to §§ 242.900 through 242.909, it must immediately upon re-opening send a message to all participants that it has resumed normal operations. Thereafter, any participant that had an obligation to report information to the registered security-based swap data repository pursuant to §§ 242.900 through 242.909, but could not do so because of the registered security-based swap data repository's inability to receive and hold in queue data, must promptly report the information to the registered security-based swap data repository.

§ 242.905 Correction of errors in security-based swap information.

(a) *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 §§ 242.900 through 242.909 shall correct such error in accordance with the following procedures:

(1) 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

(2) 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

Securities and Exchange Commission

§ 242.907

with the policies and procedures contemplated by § 242.907(a)(3).

(b) *Duty of security-based swap data repository to correct.* A registered security-based swap data repository shall:

(1) 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

(2) 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 § 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.

[80 FR 14728, Mar. 19, 2015, as amended at 81 FR 53654, Aug. 12, 2016]

§ 242.906 Other duties of participants.

(a) *Identifying missing UIC information.* A registered security-based swap data repository shall identify any security-based swap reported to it for which the registered security-based swap data repository does not have the counterparty ID and (if applicable) the broker ID, branch ID, execution agent ID, trading desk ID, and trader ID of each direct counterparty. Once a day, the registered security-based swap data repository shall send a report to each participant of the registered security-based swap data repository or, if applicable, an execution agent, identifying, for each security-based swap to which that participant is a counterparty, the security-based swap(s) for which the registered security-based swap data repository lacks counterparty ID and (if applicable) broker ID, branch ID, execution agent ID, trading desk ID, and trader ID. A participant of a registered security-based swap data repository that receives such a report shall provide the missing information with respect to its side of each security-based swap referenced in the report to the

registered security-based swap data repository within 24 hours.

(b) *Duty to provide ultimate parent and affiliate information.* Each participant of a registered security-based swap data repository that is not a platform, a registered clearing agency, an externally managed investment vehicle, or a 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 § 242.901(a)(2)(ii)(E)(4) shall provide to the registered security-based swap data repository information sufficient to identify its ultimate parent(s) and any affiliate(s) of the participant that also are participants of the registered security-based swap data repository, using ultimate parent IDs and counterparty IDs. Any such participant shall promptly notify the registered security-based swap data repository of any changes to that information.

(c) *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 § 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 §§ 242.900 through 242.909. Each such participant shall review and update its policies and procedures at least annually.

[81 FR 53654, Aug. 12, 2016]

§ 242.907 Policies and procedures of registered security-based swap data repositories.

(a) *General policies and procedures.* With respect to the receipt, reporting, and dissemination of data pursuant to §§ 242.900 through 242.909, a registered security-based swap data repository

§ 242.908

17 CFR Ch. II (4–1–23 Edition)

shall establish and maintain written policies and procedures:

(1) That enumerate the specific data elements of a security-based swap that must be reported, which shall include, at a minimum, the data elements specified in §242.901(c) and (d);

(2) That specify one or more acceptable data formats (each of which must be an open-source structured data format that is widely used by participants), connectivity requirements, and other protocols for submitting information;

(3) For specifying procedures for reporting life cycle events and corrections to previously submitted information, making corresponding updates or corrections to transaction records, and applying an appropriate flag to the transaction report to indicate that the report is an error correction required to be disseminated by §242.905(b)(2), or is a life cycle event, or any adjustment due to a life cycle event, required to be disseminated by §242.902(a);

(4) For:

(i) Identifying characteristic(s) of a security-based swap, or circumstances associated with the execution or reporting of the security-based swap, that could, in the fair and reasonable estimation of the registered security-based swap data repository, cause a person without knowledge of these characteristic(s) or circumstance(s), to receive a distorted view of the market;

(ii) Establishing flags to denote such characteristic(s) or circumstance(s);

(iii) Directing participants that report security-based swaps to apply such flags, as appropriate, in their reports to the registered security-based swap data repository; and

(iv) Applying such flags:

(A) To disseminated reports to help to prevent a distorted view of the market; or

(B) In the case of a transaction referenced in §242.902(c), to suppress the report from public dissemination entirely, as appropriate;

(5) For assigning UICs in a manner consistent with §242.903; and

(6) For periodically obtaining from each participant other than a platform, registered clearing agency, externally managed investment vehicle, or registered broker-dealer (including a reg-

istered security-based swap execution facility) that becomes a participant solely as a result of making a report to satisfy an obligation under §242.901(a)(2)(ii)(E)(4) information that identifies the participant's ultimate parent(s) and any participant(s) with which the participant is affiliated, using ultimate parent IDs and counterparty IDs.

(b) [Reserved].

(c) *Public availability of policies and procedures.* A registered security-based swap data repository shall make the policies and procedures required by §§242.900 through 242.909 publicly available on its Web site.

(d) *Updating of policies and procedures.* A registered security-based swap data repository shall review, and update as necessary, the policies and procedures required by §§242.900 through 242.909 at least annually. Such policies and procedures shall indicate the date on which they were last reviewed.

(e) A registered security-based swap data repository shall provide to the Commission, upon request, information or reports related to the timeliness, accuracy, and completeness of data reported to it pursuant to §§242.900 through 242.909 and the registered security-based swap data repository's policies and procedures thereunder.

[80 FR 14728, Mar. 19, 2015, as amended at 81 FR 53655, Aug. 12, 2016]

§ 242.908 Cross-border matters.

(a) *Application of Regulation SBSR to cross-border transactions.* (1) A security-based swap shall be subject to regulatory reporting and public dissemination if:

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

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

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

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

(v) 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.

(2) A security-based swap that is not included within paragraph (a)(1) of this section 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.

(b) *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:

(1) A U.S. person;

(2) A registered security-based swap dealer or registered major security-based swap participant;

(3) A platform;

(4) A registered clearing agency; or

(5) 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.

(c) *Substituted compliance*—(1) *General.* 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 paragraph (c)(2) of this section, 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.

(2) *Procedure.* (i) The Commission may, conditionally or unconditionally, by order, make a substituted compliance determination regarding regulatory reporting and public dissemination of security-based swaps with respect to a foreign jurisdiction if that jurisdiction's requirements for the reg-

ulatory reporting and public dissemination of security-based swaps are comparable to otherwise applicable requirements. The Commission may, conditionally or unconditionally, by order, make a substituted compliance determination regarding regulatory reporting of security-based swaps that are subject to § 242.908(a)(2) with respect to a foreign jurisdiction if that jurisdiction's requirements for the regulatory reporting of security-based swaps are comparable to otherwise applicable requirements.

(ii) A party that potentially would comply with requirements under §§ 242.900 through 242.909 pursuant to a substituted compliance order or any foreign financial regulatory authority or authorities supervising such a person's security-based swap activities may file an application, pursuant to the procedures set forth in § 240.0-13 of this chapter, requesting that the Commission make a substituted compliance determination regarding regulatory reporting and public dissemination with respect to a foreign jurisdiction the rules of which also would require reporting and public dissemination of those security-based swaps.

(iii) In making such a substituted compliance determination, the Commission shall take into account such factors as the Commission determines are appropriate, such as the scope and objectives of the relevant foreign regulatory requirements, as well as the effectiveness of the supervisory compliance program administered, and the enforcement authority exercised, by the foreign financial regulatory authority to support oversight of its regulatory reporting and public dissemination system for security-based swaps. The Commission shall not make such a substituted compliance determination unless it finds that:

(A) The data elements that are required to be reported pursuant to the rules of the foreign jurisdiction are comparable to those required to be reported pursuant to § 242.901;

(B) The rules of the foreign jurisdiction require the security-based swap to be reported and publicly disseminated in a manner and a timeframe comparable to those required by §§ 242.900

§ 242.909

through 242.909 (or, in the case of transactions that are subject to § 242.908(a)(2) but not to § 242.908(a)(1), the rules of the foreign jurisdiction require the security-based swap to be reported in a manner and a timeframe comparable to those required by §§ 242.900 through 242.909);

(C) The Commission has direct electronic access to the security-based swap data held by a trade repository or foreign regulatory authority to which security-based swaps are reported pursuant to the rules of that foreign jurisdiction; and

(D) Any trade repository or foreign regulatory authority in the foreign jurisdiction that receives and maintains required transaction reports of security-based swaps pursuant to the laws of that foreign jurisdiction is subject to requirements regarding data collection and maintenance; systems capacity, integrity, resiliency, availability, and security; and recordkeeping that are comparable to the requirements imposed on security-based swap data repositories by the Commission's rules and regulations.

(iv) Before issuing a substituted compliance order pursuant to this section, the Commission shall have entered into memoranda of understanding and/or other arrangements with the relevant foreign financial regulatory authority or authorities under such foreign financial regulatory system addressing supervisory and enforcement cooperation and other matters arising under the substituted compliance determination.

(v) The Commission may, on its own initiative, modify or withdraw such order at any time, after appropriate notice and opportunity for comment.

[80 FR 14728, Mar. 19, 2015, as amended at 81 FR 53655, Aug. 12, 2016]

§ 242.909 Registration of security-based swap data repository as a securities information processor.

A registered security-based swap data repository shall also register with the Commission as a securities information processor on Form SDR (§ 249.1500 of this chapter).

17 CFR Ch. II (4-1-23 Edition)

Regulation SCI—Systems Compliance and Integrity

SOURCE: 79 FR 72436, Dec. 5, 2014, unless otherwise noted.

§ 242.1000 Definitions.

For purposes of Regulation SCI (§§ 242.1000 through 242.1007), the following definitions shall apply:

Critical SCI systems means any SCI systems of, or operated by or on behalf of, an SCI entity that:

- (1) Directly support functionality relating to:
 - (i) Clearance and settlement systems of clearing agencies;
 - (ii) Openings, reopenings, and closings on the primary listing market;
 - (iii) Trading halts;
 - (iv) Initial public offerings;
 - (v) The provision of market data by a plan processor; or
 - (vi) Exclusively-listed securities; or
- (2) Provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets.

Electronic signature has the meaning set forth in § 240.19b-4(j) of this chapter.

Exempt clearing agency subject to ARP means an entity that has received from the Commission an exemption from registration as a clearing agency under Section 17A of the Act, and whose exemption contains conditions that relate to the Commission's Automation Review Policies (ARP), or any Commission regulation that supersedes or replaces such policies.

Indirect SCI systems means any systems of, or operated by or on behalf of, an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems.

Major SCI event means an SCI event that has had, or the SCI entity reasonably estimates would have:

- (1) Any impact on a critical SCI system; or
- (2) A significant impact on the SCI entity's operations or on market participants.

Plan processor has the meaning set forth in § 242.600(b)(67).

Responsible SCI personnel means, for a particular SCI system or indirect SCI

Securities and Exchange Commission

§ 242.1000

system impacted by an SCI event, such senior manager(s) of the SCI entity having responsibility for such system, and their designee(s).

SCI alternative trading system or *SCI ATS* means an alternative trading system, as defined in §242.300(a), which during at least four of the preceding six calendar months:

(1) Had with respect to NMS stocks:

(i) Five percent (5%) or more in any single NMS stock, and one-quarter percent (0.25%) or more in all NMS stocks, of the average daily dollar volume reported by applicable transaction reporting plans; or

(ii) One percent (1%) or more in all NMS stocks of the average daily dollar volume reported by applicable transaction reporting plans; or

(2) Had with respect to equity securities that are not NMS stocks and for which transactions are reported to a self-regulatory organization, five percent (5%) or more of the average daily dollar volume as calculated by the self-regulatory organization to which such transactions are reported;

(3) Provided, however, that such SCI ATS shall not be required to comply with the requirements of Regulation SCI until six months after satisfying any of paragraphs (1) or (2) of this definition, as applicable, for the first time.

SCI competing consolidator means:

(1) Any competing consolidator, as defined in §242.600, which, during at least four of the preceding six calendar months, accounted for five percent (5%) or more of consolidated market data gross revenue paid to the effective national market system plan or plans required under §242.603(b), for NMS stocks:

(i) Listed on the New York Stock Exchange LLC;

(ii) Listed on The Nasdaq Stock Market LLC; or

(iii) Listed on exchanges other than the New York Stock Exchange LLC or The Nasdaq Stock Market LLC, as reported by such plan or plans pursuant to the terms thereof.

(2) Provided, however, that such SCI competing consolidator shall not be required to comply with the requirements of this section and §§242.1001 through 242.1007 (Regulation SCI) until six months after satisfying any of para-

graph (1) of this definition, as applicable, for the first time; and

(3) Provided, however, that such SCI competing consolidator shall not be required to comply with the requirements of Regulation SCI prior to one year after the compliance date for §242.614(d)(3).

SCI entity means an SCI self-regulatory organization, SCI alternative trading system, plan processor, exempt clearing agency subject to ARP, or SCI competing consolidator.

SCI event means an event at an SCI entity that constitutes:

(1) A systems disruption;

(2) A systems compliance issue; or

(3) A systems intrusion.

SCI review means a review, following established procedures and standards, that is performed by objective personnel having appropriate experience to conduct reviews of SCI systems and indirect SCI systems, and which review contains:

(1) A risk assessment with respect to such systems of an SCI entity; and

(2) An assessment of internal control design and effectiveness of its SCI systems and indirect SCI systems to include logical and physical security controls, development processes, and information technology governance, consistent with industry standards.

SCI self-regulatory organization or *SCI SRO* means any national securities exchange, registered securities association, or registered clearing agency, or the Municipal Securities Rulemaking Board; *provided however*, that for purposes of this section, the term SCI self-regulatory organization shall not include an exchange that is notice registered with the Commission pursuant to 15 U.S.C. 78f(g) or a limited purpose national securities association registered with the Commission pursuant to 15 U.S.C. 78o-3(k).

SCI systems means all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance.

Senior management means, for purposes of Rule 1003(b), an SCI entity's

§ 242.1001

17 CFR Ch. II (4-1-23 Edition)

Chief Executive Officer, Chief Technology Officer, Chief Information Officer, General Counsel, and Chief Compliance Officer, or the equivalent of such employees or officers of an SCI entity.

Systems compliance issue means an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the Act and the rules and regulations thereunder or the entity's rules or governing documents, as applicable.

Systems disruption means an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system.

Systems intrusion means any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity.

[79 FR 72436, Dec. 5, 2014, as amended at 80 FR 81454, Dec. 30, 2015; 83 FR 58429, Nov. 19, 2018; 86 FR 18814, Apr. 9, 2021]

§ 242.1001 Obligations related to policies and procedures of SCI entities.

(a) *Capacity, integrity, resiliency, availability, and security.* (1) Each SCI entity shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems and, for purposes of security standards, indirect SCI systems, have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets.

(2) Policies and procedures required by paragraph (a)(1) of this section shall include, at a minimum:

(i) The establishment of reasonable current and future technological infrastructure capacity planning estimates;

(ii) Periodic capacity stress tests of such systems to determine their ability to process transactions in an accurate, timely, and efficient manner;

(iii) A program to review and keep current systems development and testing methodology for such systems;

(iv) Regular reviews and testing, as applicable, of such systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters;

(v) Business continuity and disaster recovery plans that include maintain-

ing backup and recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption;

(vi) Standards that result in such systems being designed, developed, tested, maintained, operated, and surveilled in a manner that facilitates the successful collection, processing, and dissemination of market data; and

(vii) Monitoring of such systems to identify potential SCI events.

(3) Each SCI entity shall periodically review the effectiveness of the policies and procedures required by this paragraph (a), and take prompt action to remedy deficiencies in such policies and procedures.

(4) For purposes of this paragraph (a), such policies and procedures shall be deemed to be reasonably designed if they are consistent with current SCI industry standards, which shall be comprised of information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization. Compliance with such current SCI industry standards, however, shall not be the exclusive means to comply with the requirements of this paragraph (a).

(b) *Systems compliance.* (1) Each SCI entity shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Act and the rules and regulations thereunder and the entity's rules and governing documents, as applicable.

(2) Policies and procedures required by paragraph (b)(1) of this section shall include, at a minimum:

(i) Testing of all SCI systems and any changes to SCI systems prior to implementation;

(ii) A system of internal controls over changes to SCI systems;

(iii) A plan for assessments of the functionality of SCI systems designed to detect systems compliance issues,

Securities and Exchange Commission

§ 242.1002

including by responsible SCI personnel and by personnel familiar with applicable provisions of the Act and the rules and regulations thereunder and the SCI entity's rules and governing documents; and

(iv) A plan of coordination and communication between regulatory and other personnel of the SCI entity, including by responsible SCI personnel, regarding SCI systems design, changes, testing, and controls designed to detect and prevent systems compliance issues.

(3) Each SCI entity shall periodically review the effectiveness of the policies and procedures required by this paragraph (b), and take prompt action to remedy deficiencies in such policies and procedures.

(4) Safe harbor from liability for individuals. Personnel of an SCI entity shall be deemed not to have aided, abetted, counseled, commanded, caused, induced, or procured the violation by an SCI entity of this paragraph (b) if the person:

(i) Has reasonably discharged the duties and obligations incumbent upon such person by the SCI entity's policies and procedures; and

(ii) Was without reasonable cause to believe that the policies and procedures relating to an SCI system for which such person was responsible, or had supervisory responsibility, were not established, maintained, or enforced in accordance with this paragraph (b) in any material respect.

(c) *Responsible SCI personnel.* (1) Each SCI entity shall establish, maintain, and enforce reasonably designed written policies and procedures that include the criteria for identifying responsible SCI personnel, the designation and documentation of responsible SCI personnel, and escalation procedures to quickly inform responsible SCI personnel of potential SCI events.

(2) Each SCI entity shall periodically review the effectiveness of the policies and procedures required by paragraph (c)(1) of this section, and take prompt action to remedy deficiencies in such policies and procedures.

§ 242.1002 Obligations related to SCI events.

(a) *Corrective action.* Upon any responsible SCI personnel having a reasonable

basis to conclude that an SCI event has occurred, each SCI entity shall begin to take appropriate corrective action which shall include, at a minimum, mitigating potential harm to investors and market integrity resulting from the SCI event and devoting adequate resources to remedy the SCI event as soon as reasonably practicable.

(b) *Commission notification and record-keeping of SCI events.* Each SCI entity shall:

(1) Upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred, notify the Commission of such SCI event immediately;

(2) Within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that the SCI event has occurred, submit a written notification pertaining to such SCI event to the Commission, which shall be made on a good faith, best efforts basis and include:

(i) A description of the SCI event, including the system(s) affected; and

(ii) To the extent available as of the time of the notification: The SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event; the potential impact of the SCI event on the market; a description of the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved or timeframe within which the SCI event is expected to be resolved; and any other pertinent information known by the SCI entity about the SCI event;

(3) Until such time as the SCI event is resolved and the SCI entity's investigation of the SCI event is closed, provide updates pertaining to such SCI event to the Commission on a regular basis, or at such frequency as reasonably requested by a representative of the Commission, to correct any materially incorrect information previously provided, or when new material information is discovered, including but not limited to, any of the information listed in paragraph (b)(2)(ii) of this section;

(4)(i)(A) If an SCI event is resolved and the SCI entity's investigation of