UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 100206 / May 22, 2024

ADMINISTRATIVE PROCEEDING
File No. 3-21947

In the Matter of

Intercontinental Exchange Inc., Archipelago Trading Services, Inc., New York Stock Exchange LLC, NYSE American LLC, NYSE Arca, Inc., ICE Clear Credit LLC, ICE Clear Europe Ltd., NYSE Chicago, Inc., NYSE National, Inc., and Securities Industry Automation Corporation

Respondents.

ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER

I.

The Securities and Exchange Commission ("Commission") deems it appropriate that cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 21C of the Securities Exchange Act of 1934 ("Exchange Act"), against Intercontinental Exchange Inc. ("ICE," or the "company") and certain of its subsidiaries, Archipelago Trading Services, Inc. ("ATSI"), New York Stock Exchange LLC ("NYSE"), NYSE American LLC ("American"), NYSE Arca, Inc. ("Arca"), ICE Clear Credit LLC ("ICC"), ICE Clear Europe Ltd. ("ICEU"), NYSE Chicago, Inc. ("NYSE Chicago"), NYSE National, Inc. ("NYSE National"), and Securities Industry Automation Corporation ("SIAC") (collectively, the "ICE SCI Respondents," and together with ICE, the "Respondents").

II.

In anticipation of the institution of these proceedings, Respondents have submitted an Offer of Settlement (the "Offer"), which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over them and the subject matter of these proceedings, which are admitted, Respondents consent to the entry of this Order Instituting Cease-And-Desist Proceedings Pursuant to Section 21C of the Securities Exchange Act of 1934 Making Findings, and Imposing A Cease-And-Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondents' Offer, the Commission finds that:

Summary

1. These proceedings arise out of a failure by the ICE SCI Respondents, all indirect, wholly-owned subsidiaries of ICE, to timely notify the Commission of a systems intrusion (the "Intrusion") as required by Regulation Systems Compliance and Integrity ("Regulation SCI"). The Intrusion, first identified on April 16, 2021, involved the exploitation of a "zero-day" (*i.e.*, previously unknown) vulnerability in one of Respondent ICE's virtual private network ("VPN") concentrators, networking devices that allow authorized employees to access ICE's corporate network, and indirectly ICE SCI Respondents' systems, remotely and securely.

2. The Commission adopted Regulation SCI to ensure that national securities exchanges and other SCI entities maintain their operational capability and to further the Commission's missions of protecting investors and maintaining fair and orderly markets. Among other measures, Rules 1002(b)(1) and 1002(b)(2) of Regulation SCI require that covered entities, like the ICE SCI Respondents, **immediately** notify Commission staff and also provide a written notification "[w]ithin 24 hours" when they have "a reasonable basis to conclude" that they were the subject of events constituting systems disruptions, system compliance issues or systems intrusions, as those terms are defined under Regulation SCI ("SCI events").

3. The Commission required, and emphasized the importance of, immediate notification of SCI events because any delay could hinder its ability to evaluate risk and take steps necessary to prevent harm to investors and market integrity. Accordingly, notification is required unless the covered entity also immediately concludes or reasonably estimates, pursuant to Rule 1002(b)(5) of Regulation SCI, that an SCI event had or would have no or a *de minimis* impact on the covered entity's operations or on market participants ("*de minimis*" event).

4. On April 15, 2021, a third party ("Company A") first informed ICE that it was one of several entities potentially impacted by the VPN zero-day vulnerability.

5. On April 16, 2021, the company identified malicious code associated with the threat actor that exploited the vulnerability on one of its VPN concentrators, reasonably concluding that it was, and the ICE SCI Respondents were, indeed subject to the Intrusion.

6. Over the next several days, ICE and its internal Information Security ("InfoSec") team took steps to analyze and respond to the Intrusion, including taking the compromised VPN device offline, forensically examining it, and reviewing user VPN sessions to identify any malicious sessions and/or exfiltration of data. Given the nature of the threat, the company also retained a cybersecurity firm ("Security Firm A") to conduct a parallel forensic investigation in addition to the company's internal Information Security ("InfoSec") team, and also worked with the manufacturer of the VPN device ("Company B") to confirm the integrity of ICE's network environment.

7. Five days after being notified of the vulnerability, on April 20, 2021, having uncovered no evidence of an established unauthorized VPN session or penetration of the ICE network environment, ICE InfoSec personnel determined that the threat actor's access was limited to the compromised VPN device. It was only at this point – *i.e.*, four days after first having had a reasonable basis to conclude that unauthorized entry into the concentrator had occurred, triggering the ICE SCI Respondents' immediate notification requirements to the SEC of the Intrusion – that the ICE SCI Respondents' legal and compliance personnel were finally notified of the Intrusion. And it was only at this point that the ICE SCI Respondents determined that the Intrusion was a *de minimis* event under Rule 1002(b)(5) of Regulation SCI, and that the event would therefore be reported by each of the ICE SCI Respondents in their next quarterly reports of *de minimis* SCI events.

8. The ICE SCI Respondents' failure to timely notify the Commission of the Intrusion violated Regulation SCI. Despite the Commission having established a framework under Regulation SCI mandating immediate notification of SCI systems events, the ICE SCI Respondents failed to timely contact Commission staff to provide them with notice thereof.

9. Further, ICE InfoSec personnel's failure to timely inform the ICE SCI Respondents' compliance personnel of the Intrusion violated ICE's internal cyber incident reporting procedures. For example, ICE's Cyber Incident Response Plan ("CIRP") directed that, should responsible SCI personnel[1] determine that an SCI event[2] involving a systems intrusion has occurred, "compliance and other appropriate personnel from the regulated entity must be engaged to perform the applicable Reg[ulation] SCI notification." The CIRP further emphasized that such personnel must be "notified

[1] "Responsible SCI personnel" are defined under Rule 1000 of Regulation SCI (17 CFR § 242.1000) to mean "for a particular SCI system or indirect SCI system impacted by an SCI event, such senior manager(s) of the SCI entity having responsibility for such system, and their designee(s)."

[2] One kind of "SCI event" is a "systems intrusion," which is defined under Rule 1000 of Regulation SCI (17 CFR § 242.1000) as unauthorized entry into SCI systems (*i.e.*, "any 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") or indirect SCI systems (*i.e.*, "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").

as quickly as possible after an incident is confirmed, with additional detail provided as it becomes available."

10. However, the CIRP only required legal and compliance personnel at ICE subsidiaries to be included in an "immediate e-mail alert recipient" list reserved for what the CIRP classified as "high severity" incidents (the CIRP's severity ratings went from 5 to 1, with 1 being the highest severity level). At the time of the Intrusion, "Severity 3" or "medium severity" incidents resulted in notification via e-mail of "Global Security Council" personnel, which included certain executive officers at ICE, ICE's Chief Information Security Officer ("CISO"), and members of ICE's global risk, legal, and privacy teams. For Severity 3 incidents, the CIRP did not require notification of ICE's subsidiaries' legal and compliance personnel, who were only notified by e-mail of incidents rated as "Severity 2" or "Severity 1" (i.e., "high" and "critical severity" incidents, respectively), even though the CIRP also recognized that, with respect to those incidents potentially implicating Commission notification under Regulation SCI, "[g]enerally, Severity 3 incidents are to be considered as potential de minimis SCI events, which would be reported quarterly, while Severity 2 or greater incidents, *or any systems intrusion* events are to be considered as potential immediately reportable SCI events" (emphasis added). Consequently, when members of the ICE InfoSec team designated as responsible SCI personnel[3] reasonably concluded on April 16, 2021 that the Intrusion was an SCI event and at that time assigned the Intrusion a medium severity rating, the CIRP's cyber incident escalation procedures – which were wholesale adopted by the ICE SCI Respondents – contributed to the failure by all of the ICE SCI Respondents to timely notify the Commission of the Intrusion.

11. As a result of the conduct described herein ICE caused the ICE SCI Respondents' violations of, and the ICE SCI Respondents violated, Rules 1002(b)(1) and 1002(b)(2) of Regulation SCI.

Non-Regulation SCI Covered Respondent

12. **Intercontinental Exchange, Inc. ("ICE")** is a Delaware corporation headquartered in Atlanta, Georgia, that, among other businesses, operates regulated marketplaces for the listing, trading and clearing of financial securities. ICE has a class of securities registered pursuant to Section 12(b) of the Exchange Act and is listed on NYSE under the ticker "ICE."

[3] With the exception of ICC and ICEU – which designated certain of their own employees – the ICE SCI Respondents' responsible SCI personnel for SCI events involving a systems intrusion were ICE's CISO and certain other designated InfoSec team members.

Respondents Covered by Regulation SCI (the "ICE SCI Respondents")

13. **Archipelago Trading Services, Inc. ("ATSI")** owns and operates Global OTC ("GOTC"), an alternative trading system covered by Regulation SCI. ATSI is a broker-dealer registered with the Commission pursuant to Section 15 of the Exchange Act. ATSI is a Florida corporation headquartered in Chicago, Illinois, and is an indirect, wholly-owned subsidiary of ICE. The Commission brought an enforcement action against ATSI in 2023, finding that ATSI, as the operator of GOTC, violated Section 17(a) of the Exchange Act and Rule 17a-8 thereunder. *In the Matter of Archipelago Trading Services, Inc.*, Exchange Act. Rel. No. 98234 (Aug. 29, 2023).

14. **New York Stock Exchange LLC ("NYSE")** is a national securities exchange registered with the Commission pursuant to Section 6 of the Exchange Act. NYSE is a New York limited liability company and an indirect, wholly-owned subsidiary of ICE. The Commission previously brought enforcement actions against NYSE. Most recently, in 2018, the Commission found that NYSE, American, and Arca violated Section 19(b)(1) of the Exchange Act, that NYSE and American also violated Section 17(a)(2) of the Securities Act and rules regarding business continuity and disaster recovery in violation of Rule 1001(a) of Regulation SCI, and that Arca also violated Section 19(g)(1) of the Exchange Act and Rule 608(c) of Regulation NMS. *In the Matter of New York Stock Exchange LLC, NYSE American LLC, and NYSE Arca, Inc.*, Exchange Act Rel. No. 82808 (Mar. 6, 2018). In 2014, the Commission found that NYSE, American and Arca violated Sections 19(b)(1) and 19(g)(1) of the Exchange Act. *In the Matter of New York Stock Exchange LLC, NYSE Arca, Inc., NYSE MKT LLC f/k/a/ NYSE Amex LLC, and Archipelago Securities, L.L.C.*, Exchange Act Rel. No. 72065 (May 1, 2014). In 2012, the Commission found that NYSE violated Section 17(a)(1) of the Exchange Act and Rule 17a-1 thereunder, as well as Rule 603(a) of Regulation NMS. *In the Matter of New York Stock Exchange LLC and NYSE Euronext*, Exchange Act Rel. No. 67857 (Sept. 14, 2012).

15. **NYSE American LLC ("American")** is a national securities exchange registered with the Commission pursuant to Section 6 of the Exchange Act. American currently is a Delaware limited liability company and an indirect, wholly-owned subsidiary of ICE. As noted *supra*, the Commission also brought cases against American in 2014 and 2018.

16. **NYSE Arca, Inc. ("Arca")** is a national securities exchange registered with the Commission pursuant to Section 6 of the Exchange Act. Arca is a Delaware corporation and an indirect, wholly-owned subsidiary of ICE. As noted *supra*, the Commission also brought cases against Arca in 2014 and 2018.

17. **ICE Clear Credit LLC ("ICC")** is a clearing agency registered with the Commission pursuant to Section 17A of the Exchange Act. ICC is a Delaware limited liability company and is an indirect, wholly-owned subsidiary of ICE.

18. **ICE Clear Europe Ltd. ("ICEU")** is a clearing agency that was registered with the Commission pursuant to Section 17A of the Exchange Act until November 9, 2023, at which time it became deregistered. ICEU is a UK limited company and is an indirect, wholly-owned subsidiary of ICE.

19. **NYSE Chicago, Inc. ("NYSE Chicago")** is a national securities exchange registered with the Commission pursuant to Section 6 of the Exchange Act. NYSE Chicago is a Delaware corporation and is an indirect, wholly-owned subsidiary of ICE.

20. **NYSE National, Inc. ("NYSE National")** is a national securities exchange registered with the Commission pursuant to Section 6 of the Exchange Act. NYSE National is a Delaware corporation and is an indirect, wholly-owned subsidiary of ICE.

21. **Securities Industry Automation Corporation ("SIAC")** is a New York corporation registered with the Commission as a securities information processor pursuant to Section 11A of the Exchange Act, and is an indirect, wholly-owned subsidiary of ICE.

Notification Requirements Under Regulation SCI

22. Rule 1002(b)(1) of Regulation SCI obligates SCI entities to "immediately" notify Commission staff upon responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred. Immediate notification requires that the entity make the Commission aware of the SCI event, either orally or in writing. Rule 1002(b)(2) obligates SCI entities to subsequently and within 24 hours submit a more detailed written notification regarding the relevant SCI event, though the rule is designed to provide SCI entities with flexibility by including a description of the event and the system(s) affected on a "good faith, best efforts basis," with such additional information only required to the extent available at the time.

23. The above-referenced notification requirements do not apply if an SCI entity "reasonably estimates" that, pursuant to Rule 1002(b)(5) of Regulation SCI – which includes its own separate recording and quarterly notification requirements – an SCI event has had, or would have, no or a *de minimis* impact on an SCI entity's operations or on market participants. However, unless an SCI entity reasonably estimates an SCI event to have had no or a *de minimis* impact under Rule 1002(b)(5) upon concluding that such event occurred, it must immediately notify Commission staff of the event. The Commission discussed the need for immediately notifying the Commission staff of SCI events pursuant to Rule 1002(b)(1) even when the SCI entity might not yet know the full impact or significance of a given event:

> [T]here will be instances in which an SCI entity will not know the significance of an SCI event at the time of the occurrence of an event, or whether such event (or, potentially, the aggregated impact of several SCI events occurring, for example, across many SCI entities) will warrant the Commission's input or merit the Commission's awareness, nor does the Commission believe it should be solely within an SCI entity's discretion to make such a determination. And SCI entities retain the flexibility to revise their initial assessments should they subsequently determine that the event in question was incorrectly initially assessed to be a *de minimis* event (or incorrectly initially assessed to not be a *de minimis* event).

Securities Exchange Act Rel. No.73639 (Nov. 19, 2014), 79 FR 72252 at 72324 (Dec. 5, 2014).

24. This is particularly true of systems intrusions, which by their nature may be more difficult to identify and assess as compared to other forms of SCI events.

Respondents' Policies and Procedures

25. ICE maintained certain policies and procedures intended to ensure timely internal and regulatory notification of cyber incidents. ICE's CIRP outlined the procedures to be followed by its information security personnel in the event of a cyber incident, which included systems intrusions reportable to the Commission under Regulation SCI. A dedicated ICE InfoSec team reporting to ICE's CISO handled information security responsibilities at ICE and its subsidiaries, including the ICE SCI Respondents.

26. The CIRP applied company-wide, including to all Respondents. Following the Commission's adoption of Regulation SCI, ICE modified the CIRP to refer to SCI event notification requirements. The CIRP also established a system of cyber-incident severity levels and internal notification procedures detailing how ICE and ICE SCI Respondent personnel were to be informed of the relevant cyber incident, including through an e-mail alert system requiring the notification of personnel groups at ICE and its subsidiaries based upon the assigned severity level.

27. The CIRP included criteria for cyber incidents to be ranked from 5 to 1 based on severity, with 1 being the highest severity level. "Severity 3" or "medium severity" incidents were defined as involving "unauthorized activity with targeted malicious intent, operational impact, or closure/evacuation of an ICE facility" and resulted in notification via e-mail of the company's CISO, numerous additional InfoSec personnel, and "Global Security Council" personnel, which included members of ICE's senior management and the company's global risk, legal, and privacy teams. "Severity 2" or "high severity" incidents were defined as involving "unauthorized activity with targeted malicious intent and either operational impact or physical harm." The CIRP's internal notification guidelines specifically required an e-mail alert to be sent to legal and compliance personnel at ICE's subsidiaries, including the ICE SCI Respondents as applicable, only upon assigning a Severity 2 incident rating in the company's incident tracking system.

28. Regardless of severity level, at the time that ICE identified the Intrusion on April 16, 2021, the CIRP also stated, "any systems intrusion events are to be considered as potential immediately reportable SCI events. Subsidiary compliance personnel should be notified as quickly as possible after an incident is confirmed, with additional detail provided as it becomes available…." The CIRP further required that if a cyber incident "involves a system intrusion (unauthorized entry) of a Regulation SCI or Regulation SCI-indirect system as determined by the Responsible Reg SCI Personnel, compliance and other appropriate personnel from the regulated entity must be engaged to perform the applicable Reg SCI notification."

29. Apart from the CIRP, the ICE SCI Respondents, each of which had an independent SCI event-reporting obligation, separately maintained policies specific to compliance with Regulation SCI. By way of example, GOTC, which is operated by Respondent ATSI, maintained a relevant policy document titled "Regulation SCI: Systems Events Policy & Procedures" (hereinafter "GOTC Policy & Procedures") that identified specific "Systems Intrusion Stakeholders" responsible for actively participating as needed in assessing whether or not a systems intrusion was

de minimis and preparing notifications to the Commission regarding such intrusions. Those stakeholders included, in addition to ICE's InfoSec team, GOTC's IT compliance, broker-dealer compliance, and/or legal personnel. Where ICE's CISO or an InfoSec team delegate – who GOTC named as Responsible SCI personnel – has a reasonable basis to conclude that an SCI systems intrusion event "has occurred and is not *de minimis*, and therefore immediately reportable," the GOTC Policy & Procedures required that ICE "promptly notify" GOTC's Chief Compliance Officer or a designee who, with input as needed from GOTC's legal department, will fulfill that entity's notification obligations by "immediately notify[ing] the SEC."

30. Responsible SCI personnel, however, failed to promptly notify the ICE SCI Respondents' legal and compliance personnel of the Intrusion to ensure that the ICE SCI Respondents could properly assess and fulfill their regulatory notification obligations under Regulation SCI.

The Intrusion

31. On Thursday, April 15, 2021, ICE received information from Company A that two ICE IP addresses were associated with a VPN device potentially compromised by a known threat actor. ICE InfoSec employees at that point rated the matter in ICE's incident tracking system as a "Severity 5" or "informational severity" incident, the lowest severity rating. The next day, Friday, April 16, 2021, ICE InfoSec personnel learned that, in known instances in which a target had been compromised, sophisticated threat actors, believed to be nation-state actors, installed a webshell code onto a compromised VPN device in an attempt to harvest information passing through that device, including employee name, password, and multi-factor authentication codes. This data could allow the threat actor to access internal corporate networks.

32. Using a query tool provided by Company A to locate potentially compromised VPN devices, ICE ran tests on the morning of April 16, 2021 against all of its VPN concentrators, identifying one potentially compromised device, which was classified as an indirect SCI system of each of the ICE SCI Respondents.[4] During the afternoon of April 16, 2021, ICE confirmed that the malicious webshell code was present on the identified device and determined that, as a result, the Intrusion had occurred. ICE InfoSec personnel at this time raised the severity level of the incident to "Severity 3" or "medium severity," resulting in e-mail notification to the company's CISO, additional InfoSec personnel, and members of ICE's Global Security Council.

33. ICE's InfoSec team thereafter took several measures to analyze and respond to the Intrusion. For example, by the evening of April 16, 2021, the company had retained Security Firm A to conduct an additional, parallel investigation of the Intrusion, and had both taken offline and obtained a forensic image of the compromised VPN device, which it transmitted to Security Firm A for analysis. Senior company executives and board members were informed of the Intrusion and received updates on the InfoSec team's efforts and plans to review for any signs of ICE data exfiltration. The InfoSec team also worked with Company B to confirm that no other VPN devices were compromised by the threat actor and to apply a patch provided by Company B in response to

[4] *See* n.2, above.

the VPN zero-day vulnerability to secure the affected VPN concentrator and all other similar devices from known vulnerabilities.

34. The ICE InfoSec team's investigation of the Intrusion continued into the weekend and until the following Tuesday, April 20, 2021, at which point it raised the severity level of the Intrusion to a Severity 2 or "high severity" incident after uncovering exfiltration by the threat actor of VPN configuration data and certain ICE user meta-data. The InfoSec team determined that this constituted an "operational impact" that, combined with the threat actor's malicious intent, satisfied the definition of a Severity 2 incident. The InfoSec team also concluded that the threat actor's access was isolated to the single affected VPN device after having uncovered no evidence of an established unauthorized VPN session or penetration into the ICE network environment. Security Firm A's parallel investigation continued, taking another three days to be able to confirm ICE's internal findings.

The ICE SCI Respondents' Failure to Notify the Commission Regarding the Intrusion Pursuant to Rules 1002(b)(1)-(2) of Regulation SCI

35. ICE and the ICE SCI Respondents' responsible SCI personnel did not report the occurrence of the Intrusion to the legal and compliance personnel at the ICE SCI Respondents until April 20, 2021. On that date, relevant legal and compliance stakeholders for each of the ICE SCI Respondents met with InfoSec team members to learn of the Intrusion, assess whether or not the Intrusion had no or a *de minimis* impact (*i.e.*, was a *de minimis* SCI event), and determine the appropriate Commission notification under Regulation SCI.

36. Each of the ICE SCI Respondents finally determined on April 20, 2021, that the Intrusion was a *de minimis* SCI event and internally logged the Intrusion for quarterly reporting to Commission staff pursuant to Rule 1002(b)(5).

37. On April 22, 2021, Commission staff independently contacted ICE about whether and how any of the ICE SCI Respondents had been impacted by the VPN zero-day vulnerability. ICE SCI Respondent personnel thereafter provided information to the Commission staff about the Intrusion, including that the ICE SCI Respondents had declared it a *de minimis* SCI event.

38. The ICE SCI Respondents failed to notify Commission staff of the Intrusion as specifically required pursuant to the immediate and 24-hour notification rules, Rules 1002(b)(1) and (b)(2) of Regulation SCI, respectively. The ICE SCI Respondents accordingly deprived the Commission of access to information essential to the Commission's ability to fulfill its oversight role and to protect the securities markets.

Violations

39. As a result of the conduct described above, the ICE SCI Respondents violated and ICE caused their violations of Rule 1002(b)(1) [17 C.F.R. § 242.1002(b)(1)], which requires that covered entities, 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.

40. As a result of the conduct described above, the ICE SCI Respondents violated and ICE caused their violations of Rule 1002(b)(2) [17 C.F.R. § 242.1002(b)(2)], which requires that covered entities, within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred, submit a written notification pertaining to such SCI event to the Commission.

Prior Violations by Respondents NYSE, Arca, American, and ATSI

41. In determining to accept Respondents' Offer, the Commission considered the prior Commission actions against certain Respondents, all of which are indirect, wholly-owned subsidiaries of ICE. This is the second enforcement action charging Respondents NYSE and American with violations of Regulation SCI. In 2018, the Commission charged NYSE and American with violating Regulation SCI Rules 1001(a)(1) and 1001(a)(2)(v), among other violations, finding that these entities lacked required policies and procedures for "reasonably designed" backup and recovery capabilities. That action involved additional charges against NYSE and American, as well as Respondent Arca, and followed multiple earlier enforcement actions against these entities, including a 2014 action in which the Commission found that NYSE, American and Arca violated Sections 19(b)(1) and 19(g)(1) of the Exchange Act. Most recently, in 2023, the Commission charged Respondent ATSI with violating Section 17(a) of the Exchange Act and Rule 17a-8 thereunder.

IV.

In view of the foregoing, the Commission deems it appropriate to impose the sanctions agreed to in Respondents' Offer.

Accordingly, pursuant to Section 21C of the Exchange Act, it is hereby ORDERED that:

A. Respondents shall cease and desist from committing or causing any violations and any future violations of Rules 1002(b)(1) and 1002(b)(2) of Regulation SCI.

B. Respondent ICE shall, within 14 days of the entry of this Order, pay a civil money penalty in the amount of $10,000,000.00 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717.

Payment must be made in one of the following ways:

(1) Respondent ICE may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(2) Respondent ICE may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(3) Respondent ICE may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying ICE as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Melissa R. Hodgman, Associate Director, Division of Enforcement, Securities and Exchange Commission, 100 F St., NE, Washington, DC 20549-5553.

Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondents agree that in any Related Investor Action, they shall not argue that they are entitled to, nor shall they benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondents' payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondents agree that they shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

By the Commission.

Vanessa A. Countryman
Secretary