UNITED STATES OF AMERICA
Before the
COMMODITY FUTURES TRADING COMMISSION

In the Matter of:	)	
AMP Global Clearing LLC,	)	**CFTC Docket No. 18 – 10**
Respondent.	)	

ORDER INSTITUTING PROCEEDINGS PURSUANT TO SECTION 6(c) AND (d) OF THE COMMODITY EXCHANGE ACT, MAKING FINDINGS, AND IMPOSING REMEDIAL SANCTIONS

I.

The Commodity Futures Trading Commission ("Commission") has reason to believe that AMP Global Clearing LLC ("Respondent") violated Commission Regulation ("Regulation") 166.3, 17 C.F.R. § 166.3 (2017). Therefore, the Commission deems it appropriate and in the public interest that public administrative proceedings be, and hereby are, instituted to determine whether Respondent engaged in the violation set forth herein and to determine whether any order should be issued imposing remedial sanctions.

II.

In anticipation of the institution of an administrative proceeding, Respondent has submitted an Offer of Settlement ("Offer"), which the Commission has determined to accept. Without admitting or denying any of the findings or conclusions herein, Respondent consents to the entry of this Order Instituting Proceedings Pursuant to Section 6(c) and (d) of the Commodity Exchange Act, Making Findings, and Imposing Remedial Sanctions ("Order") and acknowledges service of this Order.[1]

[1] Respondent consents to the use of the findings of fact and conclusions of law in this Order in this proceeding and in any other proceeding brought by the Commission or to which the Commission is a party or claimant, and agrees that they shall be taken as true and correct and be given preclusive effect therein, without further proof. Respondent does not consent, however, to the use of this Order, or the findings or conclusions herein, as the sole basis for any other proceeding brought by the Commission or to which the Commission is a party or claimant, other than a: proceeding in bankruptcy, or receivership; or a proceeding to enforce the terms of this Order. Respondent does not consent to the use of the Offer or this Order, or the findings or conclusions in this Order, by any other party in any other proceeding.

III.

The Commission finds the following:

A. Summary

Between June 21, 2016, and April 17, 2017 (the "Relevant Period"), Respondent, a registered futures commission merchant ("FCM"), failed to supervise diligently its information technology provider's ("IT Provider") implementation of certain provisions in Respondent's written information systems security program ("ISSP").[2] This failure left unprotected for nearly ten months a significant amount of Respondent's customers' records and information and led to the compromise of this data after Respondent's information technology network ("network") was accessed by an unauthorized third party who was unaffiliated with Respondent ("Third Party").[3] Respondent's failure to supervise its IT Provider's implementation of its ISSP and consequent failure to secure its customers' records and information violated Regulation 166.3, 17 C.F.R. § 166.3 (2017).

***

In accepting AMP's Offer, the Commission recognizes Respondent's substantial cooperation during the Commission Division of Enforcement's investigation of this matter, which included providing important information and analysis to the Division that helped the Division to efficiently and effectively undertake this investigation. The civil monetary penalty imposed on Respondent reflects Respondent's cooperation.

B. Respondent

AMP Global Clearing LLC has been registered as an FCM with the Commission since 2010. Its principal office is in Chicago, Illinois.

C. Facts

Respondent's ISSP delegates implementation of certain provisions to the IT Provider under the supervision of Respondent's officers. The relevant ISSP provisions include: (1) identifying and performing risk assessments of access routes into the network; (2) performing quarterly network risk assessments to identify vulnerabilities and reporting those results to

---

[2] Respondent adopted its ISSP pursuant to Regulation 160.30, 17 C.F.R. § 160.30 (2017), which required it to "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information." National Futures Association ("NFA") Interpretive Notice 9070, effective March 1, 2016, establishes general requirements relating to registrants' ISSPs, and Commission Staff Advisory No. 14-21, issued February 26, 2014, enumerates recommended best practices for safeguarding customers' records and information.

[3] As discussed below, the Third Party contacted federal authorities about securing the compromised information, and Respondent has represented that its internal investigation determined that the Third Party was the only unauthorized third party who accessed the compromised information.

Respondent's officers; (3) maintaining strict firewall rules to ensure access to the network only from known Internet protocol addresses; and (4) detecting unauthorized activity on the network.

1. Respondent's Network Vulnerability

On June 21, 2016, the IT Provider installed a network attached storage device ("NASD") in the network to store back-up data after recommending its purchase to Respondent. During its installation, the IT Provider did not identify that the NASD featured remote replication of its content files in real time through a software protocol known as "remote synchronization" ("Rsync"). Rsync can efficiently replicate files between NASDs over the Internet through among other means an unencrypted Internet port in the NASD ("Rsync port"). In this particular NASD series, the Rsync port was open by default, allowing permission-less access to the NASD's contents from the Internet.

Because the IT Provider did not identify or perform a risk assessment of the Rsync port while installing the NASD in accord with the ISSP, an open access route from the Internet was created through Respondent's network firewall into the NASD. Contrary to the ISSP, this left unprotected from cyber-exploitation unencrypted customers' records and information stored on the NASD. Despite this vulnerability, the IT Provider's September and December 2016 quarterly network risk assessments erroneously informed Respondent's officers that there were no network security abnormalities or concerns based on the IT Provider's periodic network penetration tests, vulnerability scans, and firewall audits.

From December 2016 through March 2017, the Third Party and his colleagues made a series of blogposts describing their access through the Rsync port to sensitive information stored on NASDs used by organizations other than Respondent, including some from the same manufacturer as relevant here. At least three of these incidents, involving commercial and government records, were subsequently reported on cybersecurity related websites and in the media. Despite these reports, the IT Provider's third quarterly network risk assessment in March 2017 again failed to identify to AMP's officers any network security concerns. In sum, contrary to the ISSP, the IT Provider failed to identify, or perform a risk assessment of the Rsync port, and failed to identify any network security concerns in its quarterly network risk assessments.

2. Compromise of Respondent's Customers' Records and Information

In late March 2017, the Third Party detected the open Rsync port in Respondent's NASD during an Internet search for network vulnerabilities. On April 10th, 2017, undetected by Respondent, the Third Party copied approximately 97,000 files from the NASD. Many of these compromised files contained Respondent's customers' records and information including personally identifiable information.

On April 17th, Respondent learned of the compromise from the Third Party and immediately removed the NASD from its network while commencing an internal investigation to assess the scope of the breach. On April 28th, Respondent reported the compromise to its customers, NFA, and the Commission. Respondent has represented that, shortly thereafter, Respondent's internal investigation determined that the Third Party was the only unauthorized third party who accessed the NASD. At approximately the same time, the Third Party contacted

federal authorities about securing the copied information. As a result of this contact, the Third Party informed Respondent that the copied information had been secured, and was no longer in the Third Party's possession.

Between June 21, 2016, and April 17, 2017, when contacted by the Third Party, Respondent was unaware that a significant amount of its customers' records and information were unprotected, that this data was subsequently compromised, and that the same deficiency had led to several compromises of sensitive information at other organizations. Although Respondent has represented that customers' records and information were not compromised beyond the Third Party, its IT Provider's failure to implement fully the ISSP left unprotected against cyber-exploitation a significant amount of customer information, over a multiple month period.

IV.

A. Legal Discussion

Regulation 166.3, 17 C.F.R. § 166.3 (2017), requires that every Commission registrant[4] "diligently supervise the handling by its partners, officers, employees and agents" of all activities relating to its business as a registrant. Regulation 166.3 imposes upon a registrant an affirmative duty to supervise its employees and agents diligently by establishing, implementing and executing an adequate supervisory structure and compliance program. *See CFTC v. Carnegie Trading Grp., Ltd.*, 450 F. Supp. 2d 788, 805 (N.D. Ohio 2006); Adoption of Customer Protection Rules, 43 Fed. Reg. 31,886, 31,889 (July 24, 1978). For a registrant to fulfill its duties under Regulation 166.3, it must both design an adequate program of supervision and ensure that the program is followed. *See, e.g.*, *In re GNP Commodities, Inc.*, CFTC No. 89-1, 1992 WL 201158, at *17-19 (Aug. 11, 1992), *aff'd sub nom. Monieson v. CFTC*, 996 F.2d 852 (7th Cir. 1993).

A violation of Regulation 166.3 is an independent violation for which no underlying violation is necessary. *See GNP Commodities*, 1992 WL 201158, at *17 n.11; *In re Paragon Futures Ass'n*, CFTC No. 88-18, 1992 WL 74261, at *13 (Apr. 1, 1992). Consequently, a violation of Regulation 166.3 "is demonstrated by showing either that: (1) the registrant's supervisory system was generally inadequate; or (2) the registrant failed to perform its supervisory duties diligently." *In re FCStone, LLC*, CFTC No. 15-21, 2015 WL 2066891, at *3 (May 1, 2015) (consent order) (citing *In re Murlas Commodities*, CFTC No. 85-29, 1995 WL 523563, at *9 (Sept. 1, 1995)); *see also Paragon*, 1992 WL 74261, at *14 (concluding that the "focus of any proceeding to determine whether Rule 166.3 has been violated will be on whether such review occurred and, if it did, whether it was 'diligent'"). Whether a registrant has met its supervisory duties is a fact-intensive determination. *See, e.g.*, *GNP Commodities*, 1992 WL 201158, at *17.

[4] An exception to this obligation exists for associated persons who do not have supervisory duties.

Regulation 160.30, 17 C.F.R. § 160.30 (2017), requires FCMs to "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."[5] An FCM may delegate the performance of its ISSP's technical provisions, including those relevant here. But in contracting with an IT Provider as its agent to perform these services, an FCM cannot abdicate its responsibilities under Regulation 166.3 and must diligently supervise the IT Provider's handling of all activities relating to the FCM's business as a Commission registrant. The protection of customers' records and information must be of paramount concern for an FCM. As noted, Regulation 160.30 requires an FCM to adopt policies and procedures to protect customer records and information. Flowing naturally from this requirement is the FCM's duty, under Regulation 166.3, to diligently supervise how those policies and procedures are implemented, and how the customer records and information are electronically protected. Here, Respondent's failure to diligently supervise the IT Provider's implementation of critical ISSP provisions constitutes a violation of Regulation 166.3. This failure is evidenced by the fact that for nearly ten months, a significant amount of Respondent's customers' records and information were unprotected and vulnerable to cyber-exploitation—a vulnerability, and ultimately a breach, of which Respondent was unaware until being notified by the Third Party.

B. Respondent's Cooperation

Respondent has represented that, upon learning of the data compromise, Respondent's officers took action to secure its customers' information and verify that the compromise was limited to the Third Party while taking additional steps to protect its network going forward. These additional steps included: (1) initiating a comprehensive review of its network security; (2) additional encryption of customers' records and information; and (3) hiring a cybersecurity firm to perform a penetration test of its network to further ensure its security. Further, Respondent provided significant cooperation to the Commission Division of Enforcement's investigation by expeditiously providing relevant records including a detailed event timeline, internal communications, and technical documents, along with the results of the penetration test of its network. These records, combined with voluntary interviews and testimony of Respondent's personnel, substantially aided the Division's reconstruction of relevant events.

Accordingly, the civil monetary penalty imposed on Respondent reflects Respondent's cooperation.

---

[5] Under NFA Interpretive Notice 9070, "each [NFA] Member must adopt and enforce a written ISSP reasonably designed to provide safeguards, appropriate to the Member's size, complexity of operations, type of customers and counterparties, the sensitivity of the data accessible within its systems, and its electronic interconnectivity with other entities, to protect against security threats or hazards to their technology systems." Similarly, Commission Staff Advisory No. 14-21 states that "[e]ach covered entity [including FCMs] should develop, implement and maintain a written information security and privacy program that is appropriate to its size and complexity" and that "[i]dentif[ies], in writing, all reasonably foreseeable internal and external risks to security, confidentiality, and integrity of personal information . . . and establish processes and controls to assess and mitigate risks, before implementing new or material changes to internal systems."

V.

FINDINGS OF VIOLATIONS

Based on the foregoing, the Commission finds that, during the Relevant Period, Respondent violated Regulation 166.3, 17 C.F.R. § 166.3 (2017).

VI.

OFFER OF SETTLEMENT

Respondent has submitted the Offer in which it, without admitting or denying the findings and conclusions herein:

A. Acknowledges receipt of service of this Order;

B. Admits the jurisdiction of the Commission with respect to all matters set forth in this Order and for any action or proceeding brought or authorized by the Commission based on violation of or enforcement of this Order;

C. Waives:

1. The filing and service of a complaint and notice of hearing;

2. A hearing;

3. All post-hearing procedures;

4. Judicial review by any court;

5. Any and all objections to the participation by any member of the Commission's staff in the Commission's consideration of the Offer;

6. Any and all claims that it may possess under the Equal Access to Justice Act, 5 U.S.C. § 504 (2012), and 28 U.S.C. § 2412 (2012), and/or the rules promulgated by the Commission in conformity therewith, Part 148 of the Regulations, 17 C.F.R. pt. 148 (2017), relating to, or arising from, this proceeding;

7. Any and all claims that it may possess under the Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. No. 104-121, §§ 201-53, 110 Stat. 847, 857-74 (codified as amended in scattered sections of 5 U.S.C. and 15 U.S.C.), relating to, or arising from, this proceeding; and

8. Any claims of Double Jeopardy based on the institution of this proceeding or the entry in this proceeding of any order imposing a civil monetary penalty or any other relief, including this Order;

D. Stipulates that the record basis on which this Order is entered shall consist solely of the findings contained in this Order to which Respondent has consented in the Offer;

E. Consents, solely on the basis of the Offer, to the Commission's entry of this Order that:

1. Makes findings by the Commission that Respondent violated Regulation 166.3, 17 C.F.R. § 166.3 (2017);

2. Orders Respondent to cease and desist from violating Regulation 166.3;

3. Orders Respondent to pay one hundred thousand dollars ($100,000), plus post-judgment interest; and

4. Orders Respondent and its successors and assigns to comply with the conditions consented to in the Offer and as set forth in Part VII of this Order.

Upon consideration, the Commission has determined to accept the Offer.

VII.

ORDER

Accordingly, IT IS HEREBY ORDERED THAT:

A. Respondent shall cease and desist from violating Regulation 166.3, 17 C.F.R. § 166.3 (2017).

B. Respondent shall pay a civil monetary penalty in the amount of one hundred thousand dollars ($100,000) ("CMP Obligation"), plus post-judgment interest, within ten (10) days of the date of the entry of this Order. If the CMP Obligation is not paid in full within ten (10) days of the date of entry of this Order, then post-judgment interest shall accrue on the CMP Obligation beginning on the date of entry of this Order and shall be determined by using the Treasury Bill rate prevailing on the date of entry of this Order pursuant to 28 U.S.C. § 1961 (2012).

Respondent shall pay the CMP Obligation by electronic funds transfer, U.S. postal money order, certified check, bank cashier's check, or bank money order. If payment is to be made other than by electronic funds transfer, then the payment shall be made payable to the Commodity Futures Trading Commission and sent to the address below:

MMAC/ESC/AMK326
Commodity Futures Trading Commission
Division of Enforcement
6500 S. MacArthur Blvd.
Oklahoma City, OK 73169
(405) 954-6569 office
(405) 954-1620 fax
9-AMC-AR-CFTC@faa.gov

If payment is to be made by electronic funds transfer, Respondent shall contact Marie Thorne or her successor at the above address to receive payment instructions and shall fully comply with those instructions. Respondent shall accompany payment of the CMP Obligation with a cover letter that identifies the paying Respondent and the name and docket number of this

proceeding. The paying Respondent shall simultaneously transmit copies of the cover letter and the form of payment to the Chief Financial Officer, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street, NW, Washington, D.C. 20581.

C. Respondent and its successors and assigns shall comply with the following conditions and undertakings set forth in the Offer:

1. Public Statements: Respondent agrees that neither it nor any of its successors and assigns, agents or employees under its authority or control, shall take any action or make any public statement denying, directly or indirectly, any findings or conclusions in this Order or creating, or tending to create, the impression that this Order is without a factual basis; provided, however, that nothing in this provision shall affect Respondent's: (i) testimonial obligations; or (ii) right to take legal positions in other proceedings to which the Commission is not a party. Respondent and its successors and assigns shall undertake all steps necessary to ensure that all of its agents and/or employees under its authority or control understand and comply with this agreement.

2. Cooperation in General: Respondent shall cooperate fully and expeditiously with the Commission, including the Commission's Division of Enforcement, in this action, and in any current or future Commission investigation or action related thereto. Respondent shall also cooperate in any investigation, civil litigation, or administrative matter related to, or arising from, this action.

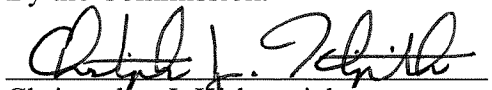
3. Required Reports: Six months and one year, respectively, from the date of the entry of this Order, Respondent shall provide a written report to the Commission: (i) detailing Respondent's efforts to maintain and strengthen the security of its network; and (ii) confirming Respondent's compliance with its ISSP's requirements.

4. Partial Satisfaction: Respondent understands and agrees that any acceptance by the Commission of any partial payment of Respondent's CMP Obligation shall not be deemed a waiver of its obligation to make further payments pursuant to this Order, or a waiver of the Commission's right to seek to compel payment of any remaining balance.

5. Change of Address/Phone: Until such time as Respondent satisfies in full its CMP Obligation as set forth in this Order, Respondent shall provide written notice to the Commission by certified mail of any change to its telephone number and mailing address within ten (10) calendar days of the change.

The provisions of this Order shall be effective as of this date.

By the Commission.



Christopher J. Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission

Dated: February 12, 2018