

II. FINDINGS

The Commission finds the following:

A. SUMMARY

During the Relevant Period, Respondent, a registered Futures Commission Merchant, failed to supervise diligently: (1) adequate implementation of and compliance with policies and procedures related to cybersecurity and the written information systems security program (“ISSP”) by its employees, including its Information Technology Systems Engineer (“IT Engineer”); and (2) adequate implementation of and compliance with policies and procedures related to customer disbursements by its employees, including its Customer Service Specialist (“Customer Service Specialist”). These failures allowed cyber criminals to breach PCI email systems, access customer information, and successfully convince PCI’s Customer Service Specialist to wire \$1 million in PCI customer funds. PCI approved reimbursement of the customer funds it had mistakenly wired to the cyber criminals within hours after discovering that it had honored a fraudulent wire request. PCI also instituted measures to preclude additional fraudulent transfers, and notified regulators that day, including the Commission’s Division of Swap Dealer and Intermediary Oversight, of the fraudulent wire request and theft. However, Respondent failed to disclose to its current customers or its prospective customers in a timely manner the material facts of the cyber breach and fraudulent wire. Respondent’s failures to supervise diligently violated Regulation 166.3, 17 C.F.R. § 166.3 (2018). Respondent’s failure to disclose material facts to its customers in a timely manner violated Regulation 1.55(i), 17 C.F.R. § 1.55(i) (2018).

B. RESPONDENT

Phillip Capital Inc. is a Futures Commission Merchant (“FCM”) and Broker Dealer based in Chicago, Illinois. PCI is part of the Phillip Capital Group, a Singapore based company that employs more than 3,500 people worldwide. PCI itself employs fewer than 35 persons.

C. FACTS

PCI employed several individuals in connection with Information Technology (“IT”), including a Senior Manager for IT Development (“IT Manager”), two software developers, and an IT Engineer. The IT Engineer was broadly responsible for data and systems issues, vendor management, website maintenance, and data archiving. The IT Engineer had limited training in cybersecurity, and cybersecurity was not broadly within the IT Engineer’s sphere of responsibility. The IT employees all reported directly or indirectly to one of the two Chief Executive Officers (“co-CEOs”). PCI’s Chief Compliance Officer (“CCO”) also had responsibility for certain IT matters, including establishing and maintaining PCI’s ISSP, and directing and overseeing PCI’s employee IT training. However, PCI’s CCO did not have a background in or familiarity with IT generally or cybersecurity specifically and was unable to adequately evaluate the sufficiency of cybersecurity policies and trainings.

PCI adopted an ISSP effective March 1, 2016, pursuant to Regulation 160.30, 17 C.F.R. § 160.30 (2018).² PCI's ISSP tracked language in NFA Interpretive Notice 9070, which provides guidance regarding information systems security practices. But PCI failed to tailor the program to its particular business activities and risks as required, and in places failed even to modify the generic language in the Notice at all.³ The ISSP identified the IT Manager as the Designated Employee with Privacy and Security Management Oversight Responsibilities ("Designated Employee"). The IT Manager gave notice of resignation in February 2018 and departed PCI two weeks later on February 23. Upon this departure, the IT Manager's position was not immediately filled; rather, PCI distributed the position's responsibilities among various PCI employees, including the IT Engineer, who were not adequately qualified to take over cybersecurity responsibilities. PCI did not at that time update the ISSP to reflect a new Designated Employee.

Moreover, PCI did not have compliance personnel who could knowledgeably assess the adequacy of its policies and procedures relating to cybersecurity. As will be described in greater detail below, this shortcoming was highlighted by PCI's failure to consult its ISSP following the cybersecurity breach, or to grasp the importance of assessing the scope of the breach and its effect on customer data.

1. Cybersecurity Breach

On February 28, 2018, PCI's IT Engineer received a phishing email from a hacked financial security organization account. The IT Engineer clicked on a PDF attachment to the email and entered login information for the PCI administrator's email account in order to access the document, unwittingly providing those credentials to cyber criminals, which they used to access the IT Engineer's email account. The IT Engineer's email account had administrator privileges, and the cyber criminals were able to use those privileges to access email accounts for PCI's co-CEO and various PCI finance employees as well. The compromised email accounts contained detailed customer information. The next day, the IT Engineer noticed that the email account had been added as a delegate to various PCI email accounts and removed the delegation. However, the IT Engineer neither reset the email account's password nor notified management. On March 2, the IT Engineer saw that the delegation removed the day before had been restored; the IT Engineer then recognized that the email account had been compromised. At that point—two days after the initial breach—the IT Engineer reset the email account's password, informed management of the breach, and at their instruction, sent an email informing all PCI employees of the email breach and directing them to change their email passwords. Upon discovery of the breach, none of the involved PCI employees—including the IT Engineer, the two co-CEOs, and the CCO—consulted the ISSP to determine responsive steps.

² Regulation 160.30 required PCI to "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information." Commission Staff Advisory No. 14-21, issued February 26, 2014, enumerated "recommended best practices" for safeguarding customers' records and information in compliance with Regulation 160.30, and National Futures Association ("NFA") Interpretive Notice 9070, effective March 1, 2016, established general requirements relating to registrants' ISSPs, and has since been updated effective April 1, 2019.

³ For example, PCI's ISSP copied verbatim the NFA language stating that "A Member's ISSP should contain a description of the Member's ongoing education and training relating to information security," rather than actually providing the description itself, and notwithstanding the fact that "Member" was not a term otherwise used or defined in PCI's ISSP.

2. Fraudulent Wire Request

On March 2, the same day that PCI management and employees learned of the email breach, the cyber criminals used customer information gleaned from the compromised emails to fraudulently extract funds. The cyber criminals sent an email to PCI, posing as a PCI customer and requesting that \$1 million be wired from that customer's omnibus account at PCI. The wire instructions identified a recipient bank account in Hong Kong, in the name of third party not otherwise known to PCI. PCI procedures required a confirmatory call to the customer when faced with this type of request. This disbursement policy was not memorialized in any formal written policy or procedure manual; rather, it was contained within a spreadsheet that PCI used to track disbursements.

Before approving the wire request, the Customer Service Specialist who received the initial email consulted a supervisor, and then the CCO, to inquire as to whether the wire was permissible. The Customer Service Specialist's inquiry made clear the employee's unfamiliarity with the relevant disbursement policy, which required a call to the customer to verify the request. Yet instead of referencing the policy, the CCO simply told the Customer Service Specialist to check whether the customer was sending funds to an account for one of its clients. The responding Customer Service Specialist replied to the fraudulent email directly to ask if the recipient in Hong Kong was a client of the PCI customer; the cyber criminals replied by email, affirming the recipient was a client and urging the Customer Service Specialist to complete the transaction. The Customer Service Specialist then approved the request, as did the finance department and other backstops within the PCI disbursement chain, and PCI wired the money out that afternoon.

PCI did not discover that the wire request was a fraud until Monday, March 5, when the defrauded customer called to ask why \$1 million had been wired from its account. Upon this discovery, PCI instituted measures to preclude additional fraudulent transfers, notified regulators that day, and within hours reimbursed its customer for the \$1 million that had been improperly disbursed.

3. Customer Notification

PCI management considered internally what, if anything, it should disclose to its customers regarding the breach and subsequent fraud. The co-CEOs ultimately determined not to inform their customers of the cybersecurity breach or the fraudulent wire transfer, and instead sent a non-specific warning to PCI customers about phishing schemes in general. From the outset, management made concerted efforts to keep the fact of the breach from its customers and the public, with one co-CEO directing staff in a company-wide email that "this is all confidential and no mention should be made outside the company – this is very important and could affect the company," and separately asking the CCO to ask any customers who may have learned of the breach not to discuss it with others, as "it will only hurt our company for others to know and it to be talked about."

Initially, PCI did not prioritize determining the impacts of the breach on customer information. In discussions with the Commission in the days and weeks following the breach, however, the Commission's Division of Swap Dealer and Intermediary Oversight repeatedly

highlighted customer disclosure obligations set forth in Commission Staff Advisory No. 14-21, expanding on the safeguarding obligations under Regulation 160.30. Only then did PCI investigate what customer information may have been compromised. PCI delegated this investigation to the IT Engineer, who was facing termination for the failures in connection with the breach, and who had no training or expertise in cybersecurity issues.

From its internal investigation, PCI discovered that the cyber criminals searched PCI email for two specific customer names, including the one under whose name they sent the fraudulent wire request. At that point—nearly two weeks after the breach—PCI first informed a second customer that its account information may have been compromised (and, in fact, the cyber criminals did subsequently make fraudulent wire requests under the name of this second customer, which PCI was able to detect). PCI further concluded that it could only identify searches that the cyber criminals had performed on certain of the compromised email accounts, but could not determine whether the cyber criminals had otherwise viewed customer information contained in the compromised accounts. Understanding that it could not know the extent of compromised customer information, PCI decided nonetheless not to inform customers whose information *may* have been compromised, on the rationale that it had no affirmative evidence that such information had in fact been viewed by the cyber criminals.

4. Post-Investigation Corrective Actions

Following the Commission’s investigation into this series of events, PCI took corrective actions to strengthen its cybersecurity defenses and improve its procedures. In addition, on February 21, 2019, PCI notified all customers for whom PCI held personally identifiable information as of March 2, 2018, about the past email breach and offered a twenty-four month membership in an identity theft monitoring service. The Commission recognizes that PCI has taken actions to correct and remediate its deficiencies on a forward-looking basis.

III. LEGAL DISCUSSION

A. Regulation 166.3

Regulation 166.3 requires that a Commission registrant, including an FCM, “diligently supervise the handling by its partners, officers, employees and agents (or other persons occupying a similar status or performing a similar function) of all commodity interest accounts carried, operated, advised or introduced by the registrant and all other activities of its partners, officers, employees, and agents (or other persons occupying a similar status or performing a similar function) relating to its business as a registrant.” 17 C.F.R. § 166.3 (2018)

The duty to supervise “include[s] the broader goals of detection and deterrence of possible wrongdoing by a [registrant’s] agents.” *Lobb v. J.T. McKerr & Co.*, CFTC No. 85R-185, 1989 WL 242384, at *11 (Dec. 14, 1989). A violation under Regulation 166.3 is an independent violation for which no underlying violation is necessary. *See In re FCStone LLC*, CFTC No. 15-21, 2015 WL 2066891, at *3 (May 1, 2015) (consent order). Consequently, a violation of Regulation 166.3 is established by showing either that: (1) the registrant’s supervisory system was generally inadequate, or (2) the registrant failed to perform its supervisory duties diligently. *FCStone*, 2015 WL 2066891, at *3 (citing *In re Murlas*

Commodities, CFTC No. 85-29, 1995 WL 523563 (Sept. 1, 1995)); *In re Paragon Futures Ass'n*, CFTC No. 88-18, 1992 WL 74261, at *14 (Apr. 1, 1992) (concluding that the “focus of any proceeding to determine whether Rule 166.3 has been violated will be on whether [a] review [has] occurred and, if it did, whether it was ‘diligent’”).

Regulation 160.30 requires FCMs to “adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information.” 17 C.F.R. § 160.30 (2018). Flowing from this requirement is the FCM’s duty, under Regulation 166.3, to supervise diligently how these policies and procedures are implemented, and how the customer records and information are electronically protected.

Here, PCI supervisors failed to adequately oversee the actions of their employees with respect to implementing and following cybersecurity policies. For example, PCI adopted an ISSP that was not reasonably tailored to its operations, and essentially copied generic NFA language. As discussed above, when the IT Manager, tasked with overseeing the ISSP, departed the firm, PCI did not then hire a replacement or assign a new employee, adequately qualified, to take over cybersecurity responsibilities. PCI also did not have compliance personnel who could knowledgably assess the adequacy of its policies and procedures relating to cybersecurity. This shortcoming was highlighted by PCI’s failure to consult its ISSP following the breach, or to grasp the importance of assessing the scope of the cybersecurity breach and its effect on customer data, even though, on its face, the ISSP protocol required PCI to identify what customer information had been accessed or misused. PCI’s failure to diligently supervise how the ISSP was implemented, and how customer records and information were electronically protected in the wake of a cybersecurity breach, constitutes a violation of Regulation 166.3

In addition to its supervision failures relating to cybersecurity, PCI also failed to supervise diligently its customer service staff in connection with disbursement policies. In particular, PCI failed to adopt or communicate to its employees clear policies and procedures for unusual disbursement requests. As evidenced by the facts described above, the Customer Service Specialist tasked with fielding disbursement requests was unfamiliar with the policy governing such situations. When the Customer Service Specialist inquired as to whether it was proper to approve the fraudulent wire request, laying bare unfamiliarity with PCI’s disbursement policies, the CCO’s directions in response were vague, inconsistent, and not made in reference to governing policies.

Consequently, PCI violated Regulation 166.3 by failing to supervise diligently adequate implementation and compliance with policies and procedures related to both cybersecurity and disbursement.

B. Regulation 1.55(i)

Regulation 1.55(i) requires FCMs to provide disclosures to existing and prospective customers that include “all information about the [FCM], including its business, operations, risk profile, and affiliates, that would be material to the customer’s decision to entrust such funds to and otherwise do business with the [FCM].” 17 C.F.R. § 1.55(i) (2018). In determining what information to disclose, the regulation specifies that the FCM should take into account “factors material to the customer’s decision to entrust the customer’s funds and otherwise do business

with the [FCM].” *Id.* An FCM “shall update the information required . . . as and when necessary, but at least annually.” *Id.*

The facts that an FCM was subject to a cybersecurity attack that compromised customer information, and then, following that attack, honored a fraudulent request to wire \$1 million in customer funds, and could not determine the scope of compromised customer information, is information that would be material to a customer’s decision to entrust its funds and do business with that FCM. Indeed, the fact that PCI took steps to safeguard these facts in order to protect its reputation demonstrates the materiality of this information. In failing to disclose this breach, PCI violated Regulation 1.55(i).

IV. FINDINGS OF VIOLATIONS

Based on the foregoing, the Commission finds that, during the Relevant Period, Respondent violated Regulations 166.3 and 1.55(i), 17 C.F.R. §§ 166.3, 1.55(i) (2018)

V. OFFER OF SETTLEMENT

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

- A. Acknowledges 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 (2018), 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, tit. II, §§ 201-253, 110 Stat. 847, 857-74 (codified as amended at 28 U.S.C. § 2412 and 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 Regulations 166.3 and 1.55(i), 17 C.F.R. §§ 166.3, 1.55(i) (2018);
 2. Orders Respondent to cease and desist from violating Regulations 166.3 and 1.55(i);
 3. Orders Respondent to pay restitution of one million dollars (\$1,000,000); however, Respondent is credited the full amount due to its previous restoration of the defrauded funds to its customer;
 4. Orders Respondent to pay a civil monetary penalty in the amount of five-hundred thousand dollars (\$500,000), plus post-judgment interest;
 5. Orders Respondent to comply with the conditions and undertakings consented to in the Offer and as set forth in Part VI of this Order.

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

VI. ORDER

Accordingly, IT IS HEREBY ORDERED THAT:

- A. Respondent shall cease and desist from violating Regulations 166.3 and 1.55(i), 17 C.F.R. §§ 166.3, 1.55(i) (2018);
- B. Respondent shall pay restitution in the amount of one million dollars (\$1,000,000) ("Restitution Obligation"). Respondent is credited the full amount due to its previous restoration of the defrauded funds to its customer, such that no further payment is owed to satisfy the Restitution Obligation.
- C. Respondent shall pay a civil monetary penalty in the amount of five-hundred thousand dollars (\$500,000) ("CMP Obligation"), plus post-judgment interest. 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 and any post judgment interest 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.

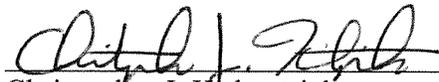
- D. Respondent shall comply with the following conditions and undertakings set forth in the Offer:
1. Public Statements: Respondent agrees that neither it nor any agents or employees under its authority or control shall take any action or make any public statement denying, directly or indirectly, any 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 shall comply with this agreement, and 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 with the Commission: 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. 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.

4. 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 calendar days of the change.
5. Undertakings: Respondent shall complete the remedial steps it has undertaken with respect to improving its cybersecurity systems and procedures, and provide a Final Report to the Commission's Division of Enforcement reflecting the completion of this process, no later than three months from the date of this Order.

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: September 12, 2019