

RECEIVED

2009 APR 29 A 6:30

REGISTRATION & DISCLOSURE

**FINANCIAL INDUSTRY REGULATORY AUTHORITY
LETTER OF ACCEPTANCE, WAIVER AND CONSENT
NO. 2007009780901**

TO: Department of Enforcement
Financial Industry Regulatory Authority ("FINRA")

RE: Centaurus Financial, Inc., Respondent
CRD No. 30833

Pursuant to FINRA Rule 9216 of FINRA's Code of Procedure, Respondent submits this Letter of Acceptance, Waiver and Consent ("AWC") for the purpose of proposing a settlement of the alleged rule violations described below. This AWC is submitted on the condition that, if accepted, FINRA will not bring any future actions against Respondent alleging violations based on the same factual findings described herein.

I.

ACCEPTANCE AND CONSENT

- A. Respondent hereby accepts and consents, without admitting or denying the findings, and solely for the purposes of this proceeding and any other proceeding brought by or on behalf of FINRA, or to which FINRA is a party, prior to a hearing and without an adjudication of any issue of law or fact, to the entry of the following findings by FINRA:

BACKGROUND

Centaurus Financial, Inc. ("CFI") has been a FINRA member since April 15, 1993. The firm conducts a general securities business with approximately 600 representatives nationwide in 300 branch offices. The firm is headquartered in Orange County, California.

RELEVANT PRIOR DISCIPLINARY HISTORY

The firm has no prior relevant disciplinary history.

OVERVIEW

Rule 30 of Regulation S-P provides that "[e]very broker, dealer . . . must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed to: (1) insure the security and confidentiality of customer records and

000057119 2009

information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.”

From April 2006 to July 2007, CFI failed to protect certain confidential customer records and information, by using an improperly configured computer firewall and employing an ineffective username and password on its computer fax server (“Computer Fax Server”). These failures permitted unauthorized persons to access stored images of faxes received by CFI, which included confidential customer information, such as social security numbers, account numbers, dates of birth and other sensitive, personal and confidential data.

CFI’s failure to adequately protect its Computer Fax Server permitted an unknown individual to conduct a “phishing” scam. When CFI became aware of the phishing scam the firm conducted an inadequate investigation and sent a misleading notification letter to affected customers and their brokers, telling them that only one benevolent person had obtained access to its Computer Fax Server. CFI also failed to maintain a supervisory system and procedures that were reasonably designed to comply with Regulation S-P. As a result of all of the above, CFI violated Reg. S-P, Rule 30 as well as NASD Rules 2110, 2210, 2211, and 3010.

FACTS AND VIOLATIVE CONDUCT

I. CFI FAILED TO ENSURE THAT IT SAFEGUARDED CONFIDENTIAL CUSTOMER INFORMATION

1. In April 2006, CFI set up its Computer Fax Server using a third party service provider so that its brokers could send customer related account documents, such as new account forms, account transfer forms, fund transfer forms and letters of authorization that contained confidential information including social security numbers, addresses and account numbers, to the Trading & Operations Department of the home office. CFI operated under the independent contractor model and had approximately 600 representatives in about 300 branch offices. Although CFI also maintained regular fax machines, it installed Internet fax service by this third party service provider to ensure that brokers could transmit time-sensitive documents to the CFI home office.

2. Using this third party service provider, CFI was able to ensure that its registered representatives and their staff would not receive a “busy” signal when trying to transmit fax communications to the Trading & Operations Department. Thus, brokers would send faxes to one phone number and such faxes would be automatically delivered through a line that was not busy at the third party service provider which would then transmit the faxes to the Computer Fax Server in the home office.

3. CFI improperly configured its firewall so that unauthorized individuals on the Internet could attempt to connect to the Computer Fax Server. At this point, if the unauthorized person had the correct username and password, that person could obtain full access to images of faxes that were stored on the Computer Fax Server which included confidential and proprietary

customer information, including account numbers, social security numbers, addresses and account balances.

4. In addition to employing a poorly configured firewall, CFI maintained a username and password that did not adequately protect the Computer Fax Server. The firm employed the username of "Administrator" and the password "password" on the Computer Fax Server. This allowed the confidential and proprietary information on the Computer Fax Server to be available to individuals who guessed the username and password and to those who utilized available technology that scans for and identifies common usernames and passwords.

II. CFI FAILED TO ADEQUATELY RESPOND TO INFORMATION THAT UNAUTHORIZED USERS HAD ACCESSED ITS COMPUTER FAX SERVER THAT CONTAINED CONFIDENTIAL CUSTOMER INFORMATION

5. On July 15, 2007, a person unknown to the firm ("Phisher") uploaded a phishing program on the Computer Fax Server ("Phishing Scam"). Phishing is a computer-based artifice designed to fool computer users into divulging personal information such as usernames, passwords, and bank and credit card information. Typically, a realistic looking, but counterfeit website is created, then a mass e-mail is sent out to recipients with a link to the counterfeit website and a request to "update" their personal information by clicking on the link provided. The files uploaded to the Computer Fax Server were designed to simulate a website for the Internet auction site eBay. The Phisher used the Computer Fax Server to host his Phishing Scam.

6. Logs of the Computer Fax Server show that the Phisher uploaded the program "eBayisapi.html" which simulated an eBay web page. Shortly after the file was uploaded, there were over 800 unauthorized logins¹ into the Computer Fax Server, most of which were the result of individuals clicking on a link provided in a mass e-mail which automatically logged them into the Computer Fax Server.

7. After the Phishing Scam was put into motion, it was posted to a "phishing" website which lists these scams in an effort to stop such activity. Certain individuals review phishing sites to determine if there are open phishing scams and notify those whose systems have been accessed or otherwise make efforts to take steps to stop such activity. One individual who reviewed phishing sites to see if there were open phishing scams contacted CFI as described below ("John Doe").

8. On Monday, July 16, 2007, one day after CFI logs show that the phishing program was uploaded by this unknown person, John Doe telephoned CFI and represented to the firm in a voicemail message that its fax server had been accessed by an unauthorized individual. John Doe's voicemail message stated that the firm's Computer Fax Server was compromised and was being used to host a phishing site. John Doe's voicemail further stated that the Computer

¹ In this AWC, the term "login" is a separate and distinct term from "download." The term "login" is used to describe a process through which an individual enters (or a computer program automatically enters) a username and password to identify the user to the computer in order to gain access to a computer or server. The term "download" describes a process in which information, data or programs are transferred from a server or host computer to one's own computer or device.

Fax Server contained "some of your customers' data that I'm sure you wanted secure." John Doe then requested that CFI contact him to obtain more details.

Subsequent to the voice message, John Doe spoke with a CFI employee and provided him the names of certain CFI server folders that John Doe stated he was able to access. At this time, the firm failed to promptly take sufficient steps to verify that its server had been accessed even though such unauthorized access was set forth on the server log.

9. On the morning of July 17, 2007, John Doe again checked CFI's Computer Fax Server to see whether it had been secured. When John Doe saw that the Computer Fax Server continued to be unprotected, John Doe downloaded² over 1800 fax images which included approximately 1400 customer fax images that contained some form of confidential customer information. John Doe then used the information he acquired to contact two CFI customers.

10. Subsequently, these two customers contacted the firm through their registered representatives notifying CFI that they had been contacted by John Doe who informed them that he had accessed their confidential and proprietary information. After acquiring John Doe's contact information from the registered representatives referenced above, a CFI compliance officer contacted John Doe to confirm his identity and verify the specific customer information that he had obtained. At this point, CFI shut down its Computer Fax Server and Internet access for the firm.

III. CFI FAILED TO CONDUCT AN ADEQUATE INVESTIGATION OF THE SCOPE OF THE UNAUTHORIZED ACCESS

11. After the firm shut down its servers, it conducted a review with the assistance of an outside technology consultant to determine the extent of unauthorized access. However, this review was inadequate. First, the review was limited to Computer Fax Server logs from July 2007. When the firm became aware that a weak username and password had been utilized, the firm should have assessed when the weak username and password were first implemented or reviewed the logs dating back to April 2006, when the Computer Fax Server was first installed. Second, while the firm's review discovered the unauthorized login related to the Phishing Scam, an adequate review would have uncovered the additional unauthorized logins into and downloads from its Computer Fax Server apparent in the July 2007 logs.

12. Centaurus failed to conduct an adequate review of the Computer Fax Server logs for the time period prior to the Phishing Scam and the ineffective firewall and username/password were in use during that period. An adequate review would have shown multiple unauthorized logins clearly apparent in the Computer Fax Server logs prior to July 2007.

IV. CFI'S FAX SERVER WAS ACCESSED BY MULTIPLE INDIVIDUALS AND WAS SUBJECT TO UNAUTHORIZED LOGINS AND DOWNLOADS

² See footnote 1.

13. Unauthorized logins to the Computer Fax Server that contained confidential and proprietary customer information began in April 2006, well prior to the Phishing Scam.

14. CFI's Computer Fax Server logs show the Computer Fax Server being scanned and a successful login established by an IP address on April 6, 2006. Beginning with this first login and continuing for more than a year until July 14, 2007, the CFI Computer Fax Server logs show the Computer Fax Server was scanned and successfully logged into 73 times by 64 unauthorized and unique IP addresses that are not associated with CFI or its third party fax service.

15. Further, after the Phishing Scam began on July 15, 2007, on just three days (July 15 through July 17, 2007), the firm's Computer Fax Server logs showed 894 unauthorized logins by 459 unique IP addresses, the vast majority of which were the result of individual recipients of the phishing e-mail clicking on a link provided in a mass e-mail which automatically logged them into CFI's computer fax server.

16. At least four unique IP addresses downloaded and/or uploaded information unrelated to the Phishing Scam. Two of these unauthorized IP addresses downloaded fax images from the Computer Fax Server on July 15-16, which contained confidential customer information. One of these IP addresses downloaded 8 files and another IP address downloaded 111 files for a total of 119 files downloaded by persons other than John Doe. The two other IP addresses uploaded unauthorized information to the Computer Fax Server.

V. CFI SENT INACCURATE NOTIFICATION LETTERS TO CUSTOMERS

17. As noted above, John Doe informed CFI that he had downloaded more than 1800 fax images. These fax images included the confidential customer information of approximately 1400 customers.

18. Most states have statutes that require customers be notified following discovery or notification of an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained. *See, e.g., CAL. CIV. CODE § 1798.82 (2008).*

19. On or about September 20, 2007, CFI sent a letter to the approximately 1400 customers whose personal and confidential information were downloaded by John Doe. The letter inaccurately stated that the unauthorized access was limited to one "benevolent" person, and the letter did not state that other unauthorized logins occurred. In addition, while stating that the intrusion was attributable to one person and that the information on the server was not openly available, the letter omitted certain facts that made those statements misleading. The letter did not inform the more than 1400 customers that the downloads were made possible due to the firm's previously inadequately configured firewall and the weak username and password. CFI was aware of the above when it sent the letter to its customers.

VI. CFI SENT INACCURATE NOTIFICATION LETTERS TO ITS REPRESENTATIVES

20. CFI also sent a substantially similar letter to the registered representatives who serviced the 1400 customers. These letters were also inaccurate as described above.

VII. CFI'S REGULATION S-P PROCEDURES

21. Rule 30 of Regulation S-P provides that "[e]very broker, dealer, and investment company, and every investment advisor registered with the Commission must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer." See 17 C.F.R. § 248.30. CFI's policies and procedures were not reasonably designed to protect confidential customer and proprietary information.

VIOLATIONS

A. INADEQUATE SUPERVISORY SYSTEM AND PROCEDURES /VIOLATION OF RULE 30 OF REGULATION S-P AND NASD RULES 3010 AND 2110 FOR AN INSECURE FIREWALL, WEAK USERNAME AND PASSWORD, AND INADEQUATE INVESTIGATION

As described above, CFI's use of a weak username and password, insecure computer firewall, as well as its inadequate investigation following notice of unauthorized access of computerized data containing confidential customer information, and CFI's inadequate supervisory procedures were not reasonably designed to comply with the federal securities laws and thus violated Reg. S-P, Rule 30 and NASD Rules 3010³ and 2110.⁴

B. INACCURATE NOTIFICATIONS TO CUSTOMERS AND REGISTERED REPRESENTATIVES /VIOLATION OF RULES 2210, 2211 AND 2110

³ NASD Rule 3010 provides in relevant part: "(a) Supervisory System. Each member shall establish and maintain a system to supervise the activities of each registered representative, registered principal, and other associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable NASD Rules. Final responsibility for proper supervision shall rest with the member. A member's supervisory system shall provide, at a minimum, for the following: (1) The establishment and maintenance of written procedures as required by paragraphs (b) and (c) of this Rule. (2) The designation, where applicable, of an appropriately registered principal(s) with authority to carry out the supervisory responsibilities of the member for each type of business in which it engages for which registration as a broker/dealer is required. (b) Written Procedures. (1) Each member shall establish, maintain, and enforce written procedures to supervise the types of business in which it engages and to supervise the activities of registered representatives, registered principals, and other associated persons that are reasonably designed to achieve compliance with applicable securities laws and regulations, and with the applicable Rules of NASD."

⁴ NASD Rule 2110 provides that "[a] member, in the conduct of his business, shall observe high standards of commercial honor and just and equitable principles of trade."

As described above, CFI gave misleading customer and representative notifications and, as such, violated NASD Rules 2210,⁵ 2211⁶ and 2110.

B. CFI consents to the imposition of the following sanctions:

1. a censure;
2. Fine in the amount of \$175,000;
3. Undertakings. CFI shall:
 - a. Disseminate corrected and accurate notifications of the unauthorized accesses noted herein, in a form not unacceptable to FINRA staff, to all previously notified customers and registered representatives within thirty (30) days of notice that this AWC has been accepted;
 - b. Offer to previously notified customers a reasonable and nationally-recognized credit monitoring service for a period of no less than one-year at no charge to the customer. This offer shall be put in writing in the notification letter noted in 3(a) above. All costs associated with the provision of credit-monitoring to previously notified CFI customers shall be born by CFI; and,
 - c. Certify by CFI's Chairman and CEO to FINRA staff within ninety (90) days from notice that this AWC has been accepted that (i) no additional unauthorized access had occurred that was not recorded in the FTP server logs (ii) that it has sent all notifications to customers as required by this AWC or applicable law; and (iii) the firm has updated and improved its Reg. S-P procedures and systems so that they are reasonably designed (a) to ensure the security and confidentiality of customer records and information (b) to protect against anticipated threats or hazards to the security or integrity of customer records and information and (c) to protect against unauthorized access to or use of

⁵ NASD Rule 2210 provides in pertinent part: "(d) Content Standards. (1) Standards Applicable to All Communications with the Public. (A) All member communications with the public shall be based on principles of fair dealing and good faith, must be fair and balanced, and must provide a sound basis for evaluating the facts in regard to any particular security or type of security, industry, or service. No member may omit any material fact or qualification if the omission, in the light of the context of the material presented, would cause the communications to be misleading. (B) No member may make any false, exaggerated, unwarranted or misleading statement or claim in any communication with the public. No member may publish, circulate or distribute any public communication that the member knows or has reason to know contains any untrue statement of a material fact or is otherwise false or misleading."

⁶ NASD Rule 2211 provides that "institutional sales material" (any communications to institutional investors) made available to "institutional investors" which includes registered representatives is "correspondence" subject to the content standards of Rule 2210 pursuant to Rule 2211(d)(1).

customer records or information that could result in substantial harm or inconvenience to any customer.

CFI agrees to pay the monetary sanctions upon notice that this AWC has been accepted and that such payment(s) are due and payable. CFI has submitted an Election of Payment form showing the method by which CFI proposes to pay the fine imposed.

CFI specifically and voluntarily waives any right to claim that CFI is unable to pay, now or at any time hereafter, the monetary sanction(s) imposed in this matter.

The sanctions imposed herein shall be effective on a date set by FINRA staff.

For good cause shown, and upon receipt of a timely written request from CFI, FINRA staff may extend any of the dates set forth above.

II.

WAIVER OF PROCEDURAL RIGHTS

CFI specifically and voluntarily waives the following rights granted under FINRA's Code of Procedure:

- A. To have a Formal Complaint issued specifying the allegations against CFI;
- B. To be notified of the Formal Complaint and have the opportunity to answer the allegations in writing;
- C. To defend against the allegations in a disciplinary hearing before a hearing panel, to have a written record of the hearing made and to have a written decision issued; and
- D. To appeal any such decision to the National Adjudicatory Council ("NAC") and then to the U.S. Securities and Exchange Commission and a U.S. Court of Appeals.

Further, CFI specifically and voluntarily waives any right to claim bias or prejudgment of the General Counsel, the NAC, or any member of the NAC, in connection with such person's or body's participation in discussions regarding the terms and conditions of this AWC, or other consideration of this AWC, including acceptance or rejection of this AWC.

CFI further specifically and voluntarily waives any right to claim that a person violated the ex parte prohibitions of FINRA Rule 9143 or the separation of functions prohibitions of FINRA Rule 9144, in connection with such person's or body's participation in discussions regarding the

terms and conditions of this AWC, or other consideration of this AWC, including its acceptance or rejection.

III.

OTHER MATTERS

CFI understands that:

- A. Submission of this AWC is voluntary and will not resolve this matter unless and until it has been reviewed and accepted by the NAC, a Review Subcommittee of the NAC, or the Office of Disciplinary Affairs ("ODA"), pursuant to FINRA Rule 9216;
- B. If this AWC is not accepted, its submission will not be used as evidence to prove any of the allegations against CFI; and
- C. If accepted:
 - 1. this AWC will become part of CFI's permanent disciplinary record and may be considered in any future actions brought by FINRA or any other regulator against CFI;
 - 2. this AWC will be made available through FINRA's public disclosure program in response to public inquiries about CFI's disciplinary record;
 - 3. FINRA may make a public announcement concerning this agreement and the subject matter thereof in accordance with FINRA Rule 8313; and
 - 4. CFI may not take any action or make or permit to be made any public statement, including in regulatory filings or otherwise, denying, directly or indirectly, any finding in this AWC or create the impression that the AWC is without factual basis. CFI may not take any position in any proceeding brought by or on behalf of FINRA, or to which FINRA is a party, that is inconsistent with any part of this AWC. Nothing in this provision affects CFI's right to take legal or factual positions in litigation or other legal proceedings in which FINRA is not a party.
- D. CFI may attach a Corrective Action Statement to this AWC that is a statement of demonstrable corrective steps taken to prevent future misconduct. CFI understands that it may not deny the charges or make any statement that is inconsistent with the AWC in this Statement. This Statement does not constitute factual or legal findings by FINRA, nor does it reflect the views of FINRA or its

staff.

CFI certifies that it has read and understand all of the provisions of this AWC and have been given a full opportunity to ask questions about it; that CFI has agreed to its provisions voluntarily; and that no offer, threat, inducement, or promise of any kind, other than the terms set forth herein and the prospect of avoiding the issuance of a Complaint, has been made to induce CFI to submit it.

3/20/09

Date

Respondent

Centaurus Financial, Inc.

By:

James R. King
[Name and title]

JAMES R. King, Chairman/CEO

Reviewed by:

Mr. Grime
Richard Grime, Esq.
Counsel for Respondent
O'Melveny & Myers
1625 Eye Street NW
Washington, D.C. 20006
(202) 383-5300

Accepted by FINRA:

4/28/09
Date

Signed on behalf of the
Director of ODA, by delegated authority

Katherine Malfa
Katherine Malfa
Vice-President
FINRA Department of Enforcement
1801 K Street NW, Suite 800
Washington, DC 20006
(202) 974-2853

CORRECTIVE ACTION STATEMENT

Centaurus Financial, Inc. ("CFI") submits this Corrective Action Statement in connection with the executed copy of the Letter of Acceptance, Waiver and Consent ("AWC"). CFI conducted an internal review of its IT systems and technologies and the procedures associated therewith. As a result of that review, CFI has made substantial hardware and software configuration changes to the Firm's network to enhance security and to protect confidential information along with significant upgrades to the physical security of the network. CFI's actions include the following measures to address the issues raised by FINRA and improve its overall compliance with the federal securities laws.

The Firm:

- installed a state-of-the-art enterprise-class firewall;
- restricted third party connectivity;
- made substantial upgrades to the physical security of the network including keycard access and door force open and ajar notifications;
- enhanced password restriction protocols for employees and administrators;
- upgraded server software;
- employed third party consultants to review firewall settings;
- performed a forensic audit and implemented recommendations to harden and secure the network;
- installed two state-of-the-art "intrusion detection devices" that identify and protect against outside threats to the network; and
- revised its Written Supervisory Procedures and Work Flow Procedures.

As such, CFI believes the issues raised by FINRA in the AWC have been addressed by the Firm in compliance with applicable rules and regulations.

This Corrective Action Statement is submitted by the Respondent. It does not constitute factual or legal findings by FINRA, nor does it reflect the views of FINRA or its staff.