CERTIFIED FINANCIAL PLANNER BOARD OF STANDARDS, INC.

ANONYMOUS CASE HISTORIES
NUMBER 30648

This is a summary of a decision issued following the October 2017 hearings of the Disciplinary and Ethics Commission ("Commission") of Certified Financial Planner Board of Standards, Inc. ("CFP Board"). The conduct at issue in this case occurred after January 1, 2009. The Rules in effect at that time under the *Rules of Conduct* were Rules 1.1 through 6.5.

I. Issues Presented

Whether a CFP® professional ("Respondent") violated CFP Board's *Standards of Professional Conduct* when she 1) conducted securities-related business communications with a firm customer using an outside/personal email account, in violation of Firm's compliance policies, which expressly stated that the use of an outside email system by a financial advisor to communicate with clients, prospects or other Firm associated persons regarding Firm business, or for any other Firm business purpose is prohibited; 2) forwarded account information for a securities customer to the same outside/personal email address, in violation of FINRA Rule 2010; and 3) failed to take prudent steps to protect the security of information and property, including the security of stored information, whether physically or electronically, that was within Respondent's control when she conducted securities-related business communications with a firm customer using an outside/personal email account.

II. Findings of Fact Relevant to the Commission's Decision

2015 CC FINRA Arbitration

Respondent met CC in January 2012 at a divorce seminar at which Respondent was speaking. Respondent, a Certified Divorce Financial Analyst ("CDFA") served as an expert witness for CC's divorce. CC trusted Respondent and decided to open an account with Firm.

CC received a $400,000 payment as part of her divorce settlement. In March 2015, these funds were held in CC's recently opened bank account at Bank. She decided to transfer the funds to Respondent and Firm for investment. In March 2015, CC received an email from Respondent's personal AOL email account. Respondent informed CC that the $400,000 Bank check that she had written to Firm could not be accepted as the check was a "starter" check.

In March 2015, CC responded to Respondent's email. She informed Respondent that she could transfer the funds in a different manner, such as a cashier's check or a wire. The same day an email from Respondent's AOL email account stated, "I highly recommend a wire transfer, attached you'll find a file with wire instructions and I'll take it from there. Let me know. Respondent." The wire instructions contained an account number for an account under the name of "Y Enterprises."

In April 2015, CC received another email from Respondent's AOL email address that stated, "I mean, is your bank going to wire the money today. Where are we in the process? Just to confirm with the accounting dept." In response to this email. CC stated, "Wire will go tomorrow. Busy day at the office […]" CC also sent an email asking if "Y Enterprises" was the right name for the recipient account. An email from Respondent's email address responded, "yes."

After confirming the wire instructions with Respondent in April 2015, the next day CC gave the wire instructions to Bank. The funds were then wired by Bank to Y Enterprises. The Y Enterprises account was

not an account for Firm, but an account used to steal the funds. The owners of the fraudulent account then wired the funds from the Y Enterprises account to accounts in China.

In April 2015, CC viewed her Firm account online. She did not see the funds, so she contacted Firm to verify receipt of the funds. The Firm representative asked CC for the wiring number which CC provided. The representative did not recognize the number. CC then contacted Respondent. At this point Respondent and CC realized that CC's funds had been stolen. CC contacted her bank, who contacted the receiving bank. The receiving bank put a freeze on the account, but the funds had already been withdrawn. CC then contacted the Sheriff's Department to report the crime.

The Sheriff's Department commenced an investigation. Respondent told the Deputy that hackers obtained unauthorized control of her personal AOL email account. Respondent told CC and the Deputy that she did not send the wiring instructions from her AOL email account. She, too, received deceptive emails from the hackers she thought were from CC, but were from a slightly modified Gmail address. The false emails Respondent received were to indicate a delay in the transfer process. Respondent confirmed to the Deputy that she routinely used the AOL email account for business.

This incident was not the first time Respondent's email had been hacked. Six months prior to the incident with CC, Respondent's email was hacked and fraudulent emails were sent to her clients. Respondent notified her clients of the situation. Respondent believed she had rectified the situation. She also contended that a computer specialist was retained by her counsel, but the specialist could not determine whose email had been hacked. Respondent stated that the computer specialist did not issue a report, since the matter settled before going to a full arbitration hearing. The Sheriff's Department completed its investigation and informed CC that recovery of her funds from China was unlikely.

Respondent contends that all parties involved were victims of the crime – CC was tricked into wiring $400,000 to a fraudulent bank account. Firm lost the ability to service CC as a client, and Respondent lost the ability to provide financial advisory services to CC.

Respondent further asserted that she should not be held solely responsible for CC's losses. She contended that the loss was caused by the criminals themselves and the banks that failed to abide by banking standards to prevent the fraud. She requested that the Arbitration Panel apportion a majority, if not all, of the fault to the actual at-fault parties and reduce any potential damages award against Respondent accordingly.

Respondent also stated that her email communications with CC using her AOL email account were known and approved by Firm. Respondent did not provide any documentation evidencing Firm's explicit approval. She claimed the AOL emails she provided to CFP Board, which was correspondence with her Firm District Manager regarding annuity illustrations demonstrated approval. She contended that to ensure her clients' information was safe and secure when communicating with them using her AOL account she changed her password frequently and used a complicated password.

In September 2016, the Arbitration was settled for $277,000. Respondent did not personally contribute to the settlement. According to Respondent, bank also participated in the final settlement, but she could not disclose the terms of bank's settlement.

2016 Firm Letter of Caution

As a result of CC's FINRA Arbitration Claim, Firm issued a Letter of Caution ("Letter") to Respondent on June 2016. Firm referenced Respondent's use of her AOL email account to communicate with CC in March 2015. Firm also noted that Respondent's use of an outside email address for Firm business was previously addressed as part of a compliance review in February 2011. The Letter reminded Respondent that Firm's compliance policies expressly state that the use of an outside email system by a financial advisor to

communicate with clients, prospects or other Firm associated persons regarding Firm business, or for any other Firm business purpose is prohibited.

Respondent objected to Firm's Letter, once again asserting that Firm knew of, and approved her use of her AOL email for work communications. Respondent later sold her Firm practice. Respondent contends that Firm did not request or require her to sell her practice – the decision was hers.

2016 FINRA Letter of Caution

In June 2016, FINRA issued a Letter of Caution to Respondent. FINRA found the following deficiency: Respondent did not comply with FINRA Rule 2010, Standards of Commercial Honor and Principles of Trade. Respondent conducted securities-related business communications with a firm customer using an outside/personal email account. Respondent also forwarded confidential account information for a securities customer to the same outside/personal email address. FINRA requested Respondent appear for a Compliance Conference, which was scheduled for June 2016.

According to Respondent, the resolution of the Compliance Conference was that she was required to write a letter to FINRA acknowledging that she understood Firm's policy regarding the use of non-firm email accounts. In her letter, Respondent also confirmed that going forward, she would not use a non-firm email account to communicate with her clients regarding Firm business.

III. Commission's Analysis and Conclusions Regarding Grounds for Discipline

First Ground for Discipline

Pursuant to Article 3(a) of the *Disciplinary Rules*, there are grounds to discipline Respondent for acts or omissions that violate Rule 3.2 of the *Rules of Conduct*, which provides that a certificant shall take prudent steps to protect the security of information and property, including the security of stored information, whether physically or electronically, that is within the certificant's control.

Respondent, a certificant, failed to take prudent steps to protect the security of information and property, including the security of stored information, whether physically or electronically, that was within the certificant's control when she conducted securities-related business communications with a firm customer using an outside/personal email account, in violation of Firm's compliance policies. Firm's compliance policies expressly state that the use of an outside email system by a financial advisor to communicate with clients, prospects or other Firm associated persons regarding Firm business, or for any other Firm business purpose is prohibited. Thus, Respondent violated Rule 3.2 of the *Rules of Conduct*.

Second Ground for Discipline

Pursuant to Article 3(a) of the *Disciplinary Rules*, there are grounds to discipline Respondent for acts or omissions that violate Rule 4.3 of the *Rules of Conduct*, which provides that a certificant shall comply with applicable regulatory requirements governing professional services provided to the client.

Respondent, a certificant, failed to comply with applicable regulatory requirements governing professional services provided to a client when she, as stated in FINRA's Letter of Caution: a) conducted securities-related business communications with a firm customer using an outside/personal email account, in violation of Firm's compliance policies; and b) forwarded account information for a securities customer to the same outside/personal email address, in violation of FINRA Rule 2010. Thus, Respondent violated Rule 4.3 of the *Rules of Conduct*.

Third Ground for Discipline

Pursuant to Article 3(a) of the *Disciplinary Rules*, there are grounds to discipline Respondent for acts or omissions that violate Rule 4.4 of the *Rules of Conduct*, which provides that a certificant shall exercise reasonable and prudent professional judgment in providing professional services to clients.

Respondent, a certificant, failed to exercise reasonable and prudent professional judgment in providing professional services to clients when she conducted securities-related business communications with a firm customer using an outside/personal email account, in violation of Firm's compliance policies. Thus, Respondent violated Rule 4.4 of the *Rules of Conduct*.

Fourth Ground for Discipline

Pursuant to Article 3(a) of the *Disciplinary Rules*, there are grounds to discipline Respondent for acts or omissions that violate Rule 5.1 of the *Rules of Conduct*, which provides that a certificant who is an employee/agent shall perform professional services with dedication to the lawful objectives of the employer/principal and in accordance with CFP Board *Code of Ethics*.

Respondent, a certificant, failed to perform professional services with dedication to the lawful objectives of the employer/principal and in accordance with CFP Board's *Code of Ethics* when she conducted securities-related business communications with a firm customer using an outside/personal email account, in violation of Firm's compliance policies. Firm's compliance policies expressly state that the use of an outside email system by a financial advisor to communicate with clients, prospects or other Firm associated persons regarding Firm business, or for any other Firm business purpose is prohibited. Thus, Respondent violated Rule 5.1 of the *Rules of Conduct*.

IV. Discipline Imposed

The Commission determined that Respondent's conduct violated Rules 3.2, 4.3, 4.4 and 5.1 of the *Rules of Conduct*, providing grounds for discipline under Article 3(a) of the *Disciplinary Rules*. After careful consideration of the record in Respondent's matter, the Commission issued to Respondent a Private Censure pursuant to Article 4.1 of the *Disciplinary Rules*. In arriving at its decision, the Commission determined that the applicable *Sanction Guidelines* recommended:

1. a Private Censure for Conduct 11: Diligence;

2. a Private Censure for Conduct 12: Employer Policy Violations; and

3. a Public Letter of Admonition for Conduct 30: Securities Law Violation.

The Commission also consulted *Anonymous Case Histories* ("ACH") 29017 and 2852. In each of these ACHs the respondent acted on information communicated to the respondent through emails that had been hacked. Each of those cases resulted in a Private Censure. Given the two ACHs, the Commission decided to give little weight to Sanction Guideline 30 because the violations at issue really were as a result of Respondent's lack of diligence in following her firm's policies. The violation of FINRA rules was simply a consequence of her lack of diligence. Given this sanction guidance, the Commission determined that the starting place for an appropriate sanction was a Private Censure. The Commission then reviewed aggravating and mitigating factors to determine if any deviation from a Private Censure was warranted.

The Commission cited in mitigation that:

1. After the first hack of Respondent's AOL email account, she changed her password to a more complex password. Respondent believed this had solved the information security problem.

2. Respondent actively participated in the search to find the hacker and worked with police to recover the stolen funds.
3. Respondent appeared to act diligently on behalf of her client as a divorce planner when she secured additional settlement proceeds that the client may not have otherwise received.
4. The harm to the client occurred primarily due to the criminal actions of others.

The Commission considered in aggravation that Respondent continued to use her AOL email account while conducting Firm business despite haven been instructed by Firm in 2011 not to do so.

Ultimately the Commission found that the mitigating factors had substantially more weight than the aggravating factor, especially the mitigating factor involving the criminal actions of others. Despite this, the Commission did not deviate downward from a Private Censure because Respondent ignored Firm's compliance rules and should have taken more prudent steps to protect the security of client information and correspondence.