Supreme Court of New Jersey
Disciplinary Review Board
Docket No. DRB 22-066
District Docket Nos. XIV-2020-0258E
and IIIB-2021-0901E

In the Matter of	:
Justin L. Scott	:
An Attorney at Law	:

Decision

Argued: September 15, 2022

Decided: October 27, 2022

HoeChin Kim appeared on behalf of the Office of Attorney Ethics.

Marc D. Garfinkle appeared on behalf of respondent.

To the Honorable Chief Justice and Associate Justices of the Supreme Court of New Jersey.

This matter was before us on a recommendation for a censure filed by the District IIIB Ethics Committee (the DEC). The formal ethics complaint charged respondent with having violated RPC 8.1(a) (three instances – making a false statement of material fact to disciplinary authorities); RPC 8.4(b) (committing

a criminal act that reflects adversely on a lawyer's honesty, trustworthiness or fitness as a lawyer in other respects); and RPC 8.4(c) (three instances – engaging in conduct involving dishonesty, fraud, deceit or misrepresentation).

For the reasons set forth below, we determine that a censure is the appropriate quantum of discipline for respondent's misconduct.

Respondent earned admission to the New Jersey bar in 2014. He has no disciplinary history and maintains a practice of law in Cherry Hill, New Jersey. During the relevant period, he was employed by Rothamel Bratton, subsequently renamed Bratton Law Group and, thereafter, Bratton Scott (collectively, the Firm), located in Haddonfield, New Jersey. Respondent's misconduct also spanned the opening of his Cherry Hill law practice in 2018.

On December 21, 2016, respondent entered into a partnership agreement (the Agreement) with the grievant, Charles Bratton, Esq., and commenced working with Bratton in January 2017. Respondent and Bratton both specialized in elder law and entered into the Agreement to unite capital and intellectual property.

According to the Agreement, respondent initially held a non-equity partner status, maintaining a seven-percent ownership interest in the Firm. The Agreement provided that respondent would accrue additional ownership interest based upon both his performance and the Firm's gross revenue. Bratton had an

unrestricted right to terminate respondent until he had obtained thirty-percent equity in the Firm. It is undisputed that respondent never obtained a thirty-percent interest during his nineteen-month tenure with the Firm.

On July 23, 2018, respondent ceased working at the Firm. The record does not clearly settle the circumstances of respondent's departure from the Firm. Bratton asserted that he fired respondent but did not disclose the basis for the termination:

> Q: Okay. How would you – how was Mr. Scott let go from your firm?
>
> A: We were in my Morristown office. I asked him to come into the office, explained to him the rationale for my terminating him. He was terminated. He was visibly upset. I again spoke to him the next day and reiterated the fact that he was terminated. And that was it.
>
> Q: And so in your view, was Mr. Scott fired then from your firm?
>
> A: Yes. That's correct.
>
> [T30.][1]

[1] "T" refers to the transcript of the December 20, 2021 formal ethics hearing.
"ExP" refers to the presenter's exhibits entered into evidence during the ethics hearing.
"RS" refers to respondent's March 4, 2022 written summation.
"OAES" refers to the OAE's March 14, 2022 written summation.
"HPR" refers to the April 26, 2022 hearing panel report.

However, respondent maintained that he left the Firm because he found Bratton difficult to work with, did not like his management style, and decided to open his own law practice.[2]

Regardless, on July 23, 2018, following his departure, the Firm disabled respondent's access to its computer system.

More than one year later, on the evening of September 20, 2019, at approximately 8:00 p.m., Matthew Bravette, Esq., a new attorney with the Firm, was working on his office desktop computer and observed an incoming connection by a program called TeamViewer.[3] Bravette described it as the "computer screen started moving without [his] input." When he took control of the mouse to toggle the cursor, the connection terminated. Bravette testified that

[2] Respondent initially told the OAE, during a demand interview, that he and Bratton determined to terminate the partnership because they viewed the practice of law differently. He offered no additional details but did state that he and Bratton each had retained counsel to address business disputes that arose as a result of the separation, including the content of letters to existing clients, but that litigation had not ensued. During the ethics hearing, respondent further explained that the separation had been contentious and that, one or two days after the separation, Bratton showed up at his home, uninvited, and shouted expletives at him. When asked why he did not tell the OAE about this altercation during his demand interview, respondent testified that he did not think it relevant.

[3] According to its website, TeamViewer is a remote access, control, and support application that provides a user remote access to computers or mobile devices. The user is required to (1) download and install TeamViewer on the device from which they wish to start the connection, such as a home computer or mobile device; (2) download and install TeamViewer on the target device, such as the office computer; and (3) enter the user's connection identification and password, thereby allowing a real time connection and control of the target device as if the user were in person. See What is TeamView?, TeamViewer, https://teamviewer.com/en-us/products/teamviewer/ (last visited October 18, 2022).

he searched for TeamViewer on his computer and found that it had a connection named "Justin Scott." Bravette's desktop computer previously had been assigned to respondent. Bravette stated that he did not use TeamViewer, was unfamiliar with that program and, until that evening, did not know it was installed on his computer. Bravette subsequently informed Bratton of what had occurred.

Bratton testified that, in response, he contacted the Firm's information technology company, Able Technology Partners (Able Technology). Able Technology commenced an investigation and confirmed that TeamViewer had been installed on that desktop.[4] Specifically, Brian Minker, a partner with Able Technology, explained:

> We confirmed that TeamViewer was installed and had been accessed several times, at which time we advised [Bratton] that he should use a company that specializes in forensics, computer forensics to take a further look at it.
>
> [T64.]

Minker also testified that he was able to "tell the software was set up and registered to Justin Scott," and that access had been made from that account

[4] To conduct its investigation, Minker explained that Able Technology examined the computer previously assigned to respondent and the computer's logs, which are made in TeamViewer and Microsoft, "that will give you a little insight of what was being done on the computer."

multiple times. Bratton subsequently retained a forensic computer company, Maragell Corporate Investigations (Maragell), and its analysis revealed respondent had accessed Bratton's computer system on at least the following six dates in 2019, all subsequent to his separation from the Firm: June 9; September 9; September 10; September 18; September 19; and September 20.[5]

Bratton permitted his employees, including respondent, to work remotely, but explained that Able Technology provided remote access via a program it endorsed, not via TeamViewer. Bratton explained that the "IT company would set up their access to the server from their home computer." Bratton testified that the Firm does not utilize TeamViewer and that he had not authorized its installation on the office computer previously used by respondent. Bratton believed respondent had installed TeamViewer, although he admittedly had not seen him do so.

Respondent testified that, when he worked remotely, he used TeamViewer rather than the remote access provided by Able Technology. He also denied using it with much frequency, stating that he used it if "it were a snow day." Respondent denied having installed TeamViewer on his former desktop

[5] Although the Maragell report was attached to the grievance and admitted into evidence, neither party called a representative of Maragell to testify at the hearing.

computer. Rather, respondent claimed that Able Technology had installed TeamViewer on his desktop computer, with Bratton's knowledge:

> Q: Your testimony was that you did not register the version of TeamViewer that was on the desktop at the Bratton firm?
>
> A: All I know is Able – Able installed that. They (indiscernible) deny it, but they put on there the ability to login to the computer remotely.
> . . .
>
> Q: How, then, were you able to – how did you know TeamViewer was available on your desktop in the office at the Bratton firm if you didn't download it?
>
> A: Because some – someone with Able put it on there and that's how I was coached to use it.
>
> [T142.]

Respondent told the OAE, during his November 16, 2020 demand interview, that Bratton had encouraged him to explore remote work and that he "ran with the idea and worked with Able Technologies." Respondent further claimed that Bratton would have been billed for the installation of TeamViewer, and that he possessed e-mails with the Firm's officer manager that would corroborate his position that the Firm was aware of his TeamViewer usage:

> Q: So there should be some sort of payment made from Bratton Scott to Able Technology regarding TeamViewer?
>
> A: That's correct.

[ExP-9p24.]

Following his interview, on November 17, 2020, the OAE requested that respondent produce the corroborating documentation. In reply, respondent produced only the following two e-mails:

(1) **July 18, 2018** e-mail from Robert Bondy, of Able Technology, stating "Justin I would like to start your new laptop configuration this afternoon. Would this work for you? If not please let me know a good day and time;"[6] and

(2) **August 18, 2017** e-mail exchange between respondent and Tina Lutts (who respondent had claimed was an officer manager with the Firm) [7] in which respondent asked, "Can you turn my computer on so I can access it remotely? Thanks!" Lutts replied, "It is on." Respondent then asked "Can you turn on teamviewer? Says team viewer is not running." Lutts did not reply.

[6] Minker explained that Able Technology would assist with setting up a personal laptop to be used for remote access, but that the "configuration" did not include the installation of TeamViewer.

[7] Lutts did not testify at the ethics hearing. In his testimony, Bratton explained that Lutts was not an office manager, but rather an estate planning paralegal who does not determine or keep track of who has remote access. According to her public profile on the Firm's website, Lutts is described as a Senior Estate Planning Paralegal. See Our Team, Bratton Law Group, https://www.brattonlawgroup.com/our-team/ (last visited September 27, 2022). A prior version of the website identified Jeffrey Lyons as the Firm's office manager. See Our Team, Bratton Law Group, https://www.brattonlawgroup.com/our-team/ (visited August 5, 2022).

Respondent claimed that the e-mails would "dispel the notions that [r]espondent may have installed the 'spy' program without [Bratton's] knowledge or that he did so in anticipation of his departure."

Able Technology confirmed that it had no record of ever having installed, or worked with, TeamViewer at the Firm. Specifically, Minker, who testified on behalf of Able Technology, stated that his company had provided information technology services to the Firm since April 2017. He confirmed that his company does not regularly use TeamViewer and did not install TeamViewer on any of Bratton's office computers. Further, he confirmed that his company had not installed TeamViewer on respondent's personal computers.

Moreover, Minker confirmed that he had reviewed Able Technology's business records and possessed no written documentation of having installed TeamViewer on any Bratton office computer or having been paid for doing so. Specifically, in his December 4, 2020 letter to Bratton, Minker stated:

> I've searched our database of charges and found no reference to us ever installing or working with TeamViewer at your company until the issue arouse [sic] regarding unauthorized access in September of last year.
>
> [ExP-15.]

Further, Able Technology's inspection of respondent's former desktop revealed that a free version of TeamViewer had been installed, which was not

licensed for commercial use. Able Technology provided three reasons why it "would never install TeamViewer," even if requested to do so:

> First, the free version (like the one found on [respondent's] former computer) is not licensed for commercial use. Second, we already have a licensed, enterprise grade, audit enabled remote access solution on all company computers that we use for remote support and can share with users if they need remote access. Third, we would not set up any access based on a user's personal account, TeamViewer or otherwise.
>
> [ExP-15.]

Minker further explained that Able Technology relied upon its own support tools, rather than a program like TeamViewer, because its own system "has a very robust monitoring" system which allows Minker to audit remote access by any user.

Last, Minker testified that if, hypothetically, Able Technology used and installed the TeamViewer program, it would do so in its own name (or that of the Firm) and not that of the individual user:

> I don't think we would ever use it. But if we did, we would want to have control over it because we need to be able to lock people out. We need to be able to, you know, diagnose problems. But, generally, the remote software is going to either be owned by the firm or it's going to be owned and controlled by us.
>
> [T67.]

Minker acknowledged, on cross-examination, that, although the computer logs revealed that respondent had accessed his former desktop computer, during and subsequent to his employment with the Firm, those same logs did not reveal who had installed TeamViewer on respondent's former office desktop.

As previously noted, at the recommendation of Able Technology, Bratton engaged Maragell, a forensic computer company, to examine respondent's former desktop. On December 10, 2019, Maragell issued its report and concluded that respondent had logged into his former office desktop via TeamViewer on six dates, all subsequent to his separation from the Firm. Maragell stated in its report that by "logging into the Desktop, [respondent] had the opportunity to view data within the Time Matters program and any other application on the Desktop and anywhere the Desktop was authorized to go (i.e. the firm's server, other connected firm computers)." As part of its analysis, Maragell also examined whether respondent had copied or transferred any files and determined that he had not done so.

Ultimately, respondent admitted that he repeatedly had accessed Bratton's computer system, using the TeamViewer program, following his separation from the Firm. His claimed motivation for doing so, however, evolved over the course of the OAE's investigation. Initially, on March 23, 2020, respondent, through

his attorney, portrayed his remote access to Bratton's computer system as accidental:

> [respondent] maintains that he had no intention to enter the BrattonScott portal on any of the occasions that were reported by Mr. Brennan, the forensic investigator.
>
> [ExP-3.]

Respondent claimed that when he started his new law firm, he utilized the same technology services that he had used while employed at the Firm, including the use of TeamViewer. Once TeamViewer was installed on his new devices, however, he claimed there were two TeamViewer portals because he had never removed the portal used to access Bratton's computer system.[8] Respondent's attorney, thus, maintained that:

> [b]ecause he now had two accounts with TeamViewer, he had two portals and, according to him, it was impossible for him to know, upon logging in, which computer he would enter. He sometimes erred. Those are the visits which troubled Mr. Bratton.
>
> [ExP-3.]

[8] Respondent told the OAE that he hired Able Technology when he started his new law firm, and that Able Technology installed TeamViewer on respondent's new computer system in late 2018 or early 2019. Minker, however, denied that respondent had retained Able Technology, although he believed his firm may have submitted a proposal for the work. Minker further denied ever having installed TeamViewer on any of respondent's computers.

Although "[h]e had no need or intention to access the BrattonScott computer," respondent kept his portal because "[h]e thought that it might become necessary in the future for him to access the BrattonScott computer to serve those clients of his who followed him to his new firm."

On August 24, 2020, five months after having told the OAE that his access to Bratton's computer system had been inadvertent, respondent admitted that his access had been intentional. Specifically, respondent explained his motivation as follows:

> I was trying to build my new practice. When I was in his computer, I was mostly interested in seeing how Mr. Bratton's practice was doing.
>
> I think it is fair to say that each and every login by me was to see what I could learn regarding Mr. Bratton's calendar and who was referring business to him. Typically, I would search specific names to see which professionals were referring clients to him.
>
> When I went into Mr. Bratton's system, I often checked the calendar day by day to see what his activities were. I would also go through the various staff members to see who was busy and who wasn't. I had no intention of removing or copying anything of value; my goal was to sit on my couch and compare Mr. Bratton's week to mine.
>
> I also searched Matt's email a few times as well to see what other professionals had emailed him.
>
> [ExP-6.]

Subsequently, on November 16, 2020, during the OAE's interview, respondent admitted that he had accessed the Firm's computer system via TeamViewer approximately six times but asserted that he believed he was authorized to do so "because it was under Bratton Scott LLC."

> Q: Okay. When you accessed your desktop remotely, and this is after you've left Mr. Bratton did you have permission to access that?
>
> A: I believe that I did at the time because it was under Bratton Scott LLC.
>
> Q: Okay. Do you – I'm sorry, this is after you left the firm?
>
> A: That is correct.
>
> Q: And you for some reason thought you still have access? Why did you think you still had access?
>
> A: At the time we were in a lawsuit between us, he and I, because we had some discrepancies on how the business would end, such as sending out a letter to all of the former clients and being able to let the clients decide whether they would chose [sic] to stay with Mr. Bratton or chose [sic] to stay with me. So when I had originally discovered the access point, I had used that to – I just looked at his calendar is what I looked at just to see how busy he was.
>
> [ExP-9pp11-12.]

Respondent also claimed that Able Technology had installed TeamViewer on his personal laptop, not his office computer, and that he had told Bratton of the installation. Those claims were unsupported by documentation. Respondent

maintained that, when he opened TeamViewer, it had saved the login credentials he utilized while employed by the Firm, thereby allowing access after his separation from the Firm:

> Q: Okay. And then when you opened up your own firm, what happened again?
>
> A: So when you click through Team Viewer, Team Viewer has my credentials saved to access Bratton Scott. So it logged into Bratton Scott, and that's how I had done it before. So he hadn't shut me out of that piece of technology.
>
> [ExP-9p16.]

Respondent admitted that his unauthorized entries into Bratton's computer system provided him access to the server, files, and client information. However, he denied having accessed anything other than Bratton's and various staff members' calendars and e-mail accounts. During the ethics hearing, respondent reiterated that he "just wanted to know what [Bratton] was doing for the week," so he looked at the calendar to "see how many consults he had versus how many consults [respondent] had."

> I wanted to know what his week looked like compared to mine. The biggest reason was because he has a marketer there that was trashing my name, and I just wanted to know who was actually referring to me versus him.
>
> [T128.]

He attributed his decisions to his competitive character and described his conduct as having "fell into stupid."

Respondent asserted that, on the six occasions when he accessed Bratton's computer system following his termination, he had difficultly staying logged on, was granted access for five-minute intervals, and had to repeatedly log back on to access the calendar. Respondent admitted that he had access to Bratton's client lists but denied using them for any purpose. Respondent also denied having access to any client medical records, personal or professional e-mails, or marketing materials.

Bratton, on the other hand, testified that he believed respondent used the confidential client information he had obtained as a result of his unauthorized access to his computer system to pursue clients. In support of his contention, Bratton asserted that he had received a telephone call, on July 18, 2019, from an existing client, who informed him that respondent and Cynthia Sharp, Esq., showed up at her home following her husband's funeral. Respondent denied going to the client's home but admitted he had worked with Sharp while setting up his new law office. Respondent explained that Sharp previously had been affiliated with Bratton's law firm and had represented the client, and that he believed the client was interested in Sharp's continued representation. Respondent denied, however, obtaining any information regarding the client,

including her address, via his unauthorized access to Bratton's computer system. The OAE was unable to interview the client.

Bratton also provided an August 3, 2018 e-mail from another client, which stated that she and her sisters had been contacted by respondent, despite Bratton's representation to her that respondent would not have access to the client's files or family contact information following his separation from the Firm. Respondent denied having improperly contacted the client but admitted that he contacted her within the first week of his separation from the Firm believing she may want to keep him as her attorney.

Bratton also testified to having learned that a third client had been contacted by respondent, but could not recall the date, other than it occurring after respondent's July 2018 termination.[9]

Bratton admitted, however, that his computer forensic company was unable to determine what client files, if any, respondent had remotely accessed or whether client files had been copied.

Based on the foregoing facts, respondent stipulated to having violated RPC 8.1(a); RPC 8.4(b); and RPC 8.4(c) but disagreed regarding the number of instances of his misconduct.

[9] Bratton conceded that respondent could have accessed client information prior to his separation from the Firm.

Specifically, respondent stipulated to having violated RPC 8.1(a) and RPC 8.4(c) by initially misrepresenting to the OAE that he had not intentionally accessed Bratton's computer system following his separation from the Firm, and RPC 8.4(b) by accessing Bratton's computer system after his separation from the Firm, in violation of N.J.S.A. 2C:20-25(a) and N.J.S.A. 2C:20-25(e).[10]

Respondent denied having violated RPC 8.1(a) in connection with the other charged instances.[11] Specifically, respondent asserted he had not been terminated by Bratton but, rather, had left on his own accord. Thus, he argued that he could not have violated the Rules of Professional Conduct by having denied to the OAE that Bratton terminated his employment. Likewise, respondent claimed that he did not install TeamViewer on his computer while at the Firm and, therefore, could not have violated the RPCs by denying this fact.

[10] Respondent was not criminally charged for his misconduct. Prior to filing his ethics grievance, Bratton contacted the Haddonfield Police Department to file a criminal complaint but was told that the matter appeared to be civil and not criminal.

[11] The complaint charged respondent with having made a false statement of material fact to the OAE, in violation of RPC 8.1(a), in three instances, when:

> (1) he denied he was terminated from the Firm;
> (2) he represented that Able Technology installed TeamViewer on his computer while at the Firm; and
> (3) he represented that he had not intended to access the Firm's computer system when he used TeamViewer after his termination.

Respondent also denied having violated RPC 8.4(c) under the other theories charged in the complaint.[12] Although respondent admitted to having unlawfully accessed Bratton's computer system, in violation of RPC 8.4(b), he denied that it constituted conduct involving fraud, dishonesty, deceit or misrepresentation. Further, respondent denied having installed TeamViewer on his computer and argued that he, thus, could not have violated the RPCs when he represented to the OAE that he had not installed the program on his computer while employed by the Firm.

In his March 4, 2022 written summation, respondent, through counsel, readily admitted to his unauthorized intrusions into the Firm's computer system, but claimed he was solely motived by his curiosity regarding Bratton's workload. Respondent further asserted that:

> There was no evidence that [r]espondent removed or copied the files, client information or documents of any sort. Respondent's testimony was that he was driven by his competitive nature to verify [Bratton's] calendar for indications of how busy that office was. Your Honor's recommendation as to discipline should reflect that.

[12] The complaint charged respondent with having engaged in conduct involving dishonesty, fraud, deceit and misrepresentation, in violation of RPC 8.4(c), when:

(1) he accessed the Firm's computer system after his termination;
(2) he misrepresented to the OAE that he had not installed TeamViewer on his computer while employed at the Firm; and
(3) he misrepresented to the OAE that he had not accessed the Firm's computer system after his separation from that firm.

> Respondent denies the claim that he wrongfully contacted any of the firm's present or former clients for the purpose of offering his services. While there were a few enumerated contacts with firm clients, the OAE failed to produce clear and convincing evidence that any of those contacts involved unethical means or otherwise constituted solicitation in violation of the Rules or the RPCs.
>
> [RSp2.]

In turn, the OAE asserted that the evidence clearly and convincingly established that respondent had violated the RPCs in all charged instances. Concerning his termination from the Firm, the OAE relied upon the Agreement that vested Bratton with absolute discretion to terminate respondent until such time as he had gained a thirty-percent interest in the partnership. The OAE emphasized in its summation that, at the time of separation, respondent had attained only a seven-percent interest in the Firm and, thus, Bratton was contractually permitted to terminate the relationship.

With respect to respondent's installation of TeamViewer on his former desktop computer, the OAE relied upon the testimony of Bratton, who unambiguously stated he did not authorize the installation of TeamViewer on the Firm's computers. The OAE also relied upon Minker's corroborating testimony that his company does not use TeamViewer and had not installed TeamViewer on a Firm computer. As further evidence that respondent, and not Able Technology, had installed the TeamViewer program, the OAE relied upon

the fact that the investigation by Able Technology revealed that a free version of the TeamViewer program had been installed, rather than the commercial version that Able Technology would have been used in a professional setting. Further, if Able Technology had installed TeamViewer or been aware of its presence, as respondent claimed, it would have disabled respondent's access in the same way it disabled respondent's other access to Bratton's computer system following his separation from the Firm. Based upon the foregoing, the OAE asserted that it had presented clear and convincing evidence that respondent had lied about being fired from the Firm, and had lied about having installed TeamViewer, in violation of RPC 8.1(a). Under the same theory, respondent's misrepresentation to the OAE concerning his installation of TeamViewer also violated RPC 8.4(c).

The OAE further asserted that respondent engaged in conduct involving dishonesty, fraud, deceit or misrepresentation, violative of RPC 8.4(c), in a third respect, by illegally gaining access to the Firm's computer system containing confidential client information.

> Simply stated, respondent no longer had any authority to access the information contained in the Bratton firm's computer system. Using TeamViewer, after his termination in July 2018, enabled respondent to view otherwise confidential information about his former firm's activities. That conduct was not honest, but rather, was deceitful, fraudulent, and misrepresented

> the fact he had been shut out of the Bratton firm's system since July 2018.
>
> [OAESp5.]

Citing In re Alper, 242 N.J. 143 (2020), discussed below, the OAE argued that respondent's misconduct warranted at least a censure, notwithstanding his lack of any prior discipline.

> Here, respondent accessed the computer system of his former employer without authority after he had been terminated, which is a grave offense as lawyers deal with confidential and privileged client information. Although respondent couched his forays as curiosity about grievant's schedule, with no nefarious purpose, the OAE counters that any unauthorized access is nefarious. As stated by Bratton, respondent's accessing his firm's computer system was equivalent to respondent's physical breaking into the premises of his law office.
>
> [OAESp6.]

Based upon the testimony and evidence presented, the DEC found, by clear and convincing evidence, that respondent violated RPC 8.1(a); RPC 8.4(b); and RPC 8.4(c) (two instances).

Specifically, the DEC concluded that respondent violated RPC 8.1(a) by falsely stating, in his March 23, 2020 letter to the OAE, that he did not intend to access the Firm's computer system after his July 23, 2018 separation from the Firm. The DEC emphasized respondent's subsequent admission that he had intentionally and repeatedly accessed Bratton's computer system following his

separation from the Firm. The DEC did not, however, find clear and convincing evidence that respondent had separately violated RPC 8.1(a) by denying that he was terminated by Bratton, or by claiming Able Technology had installed TeamViewer on his computer while he was employed by Bratton.

Specifically, the DEC referenced respondent's March 23, 2020 letter to the OAE which stated, in part, "Mr. Scott found Mr. Bratton to be unreasonable at times, as a result, he left that firm and created his own law practice, ScottCounsel. Mr. Scott was never terminated from BrattonScott in the sense that lawyers use, but that distinction may have little bearing here." The DEC determined that this letter, standing alone, failed to demonstrate whether respondent's "quibbling over whether his affiliation with BrattonScott, which firm bore his name, ended by a separation driven in part by his frustrations with Mr. Bratton or whether [r]espondent's denial that he was 'terminated' from BrattonScott was a knowingly false statement of material fact in violation of RPC 8.1(a)."

The DEC also determined that the record did not clearly and convincingly establish who had installed TeamViewer on respondent's former office computer and, in the absence of such evidence, it could not find that respondent had lied to the OAE by stating that Able Technology had installed the program. The DEC acknowledged Minker's testimony that Able Technology did not

utilize TeamViewer and had not installed it but noted the fact that Minker was unable to confirm that respondent had installed the TeamViewer program.

The DEC also determined that the evidence supported respondent's admission to having violated RPC 8.4(b) by engaging in criminal activity, in violation of N.J.S.A. 2C:20-25(a) and N.J.S.A. 2C: 20-25(e), by knowingly and repeatedly accessing Bratton's computer system after July 23, 2018, when he was no longer authorized to do so.

The DEC further determined that respondent also violated RPC 8.4(c), in two respects, by accessing Bratton's computer system after his separation from the Firm, and by lying to the OAE about having done so. Because the evidence did not clearly and convincingly establish who installed the TeamViewer program on respondent's desktop computer, however, the DEC determined that respondent did not separately violate RPC 8.4(c) by representing to the OAE that Able Technology had installed TeamViewer.

Citing Alper, the DEC recommended a censure as the proper quantum of discipline. In aggravation, the DEC found that respondent had shown little remorse for his actions.

> The Panel considered the frequency and duration of his unauthorized access, the seriousness of [r]espondent's conduct, his subsequent lies to deny his responsibility, and his overall demeanor during the hearing in which he attempted to downplay the significance of his misconduct. In re Pena, 164 N.J. 222, 234 (2000).

[HPRpp15-16.]

In mitigation, the DEC noted that respondent had no prior discipline and had not injured any client by his misconduct. However, the DEC rejected respondent's contention that his conduct was not for personal gain, and that the circumstances showed little likelihood of repeating themselves, particularly given, in the DEC's view, respondent's lack of remorse and his lies to the OAE. Further, in light of the recency of his misconduct, the DEC accorded little weight to respondent's claimed "exemplary conduct since his violations" underlying this matter.

At oral argument before us, the OAE reiterated its agreement with the DEC's recommendation that respondent be censured for his misconduct. However, the OAE urged us to find, contrary to the DEC's determination, that the evidence clearly and convincingly established that respondent had violated all the charged RPCs.

Similarly, during oral argument, respondent, through his counsel, agreed that his lack of candor had made a censure "inevitable," but characterized a term of suspension as unnecessary. Respondent's counsel also acknowledged, in response to our inquiry, that the record lacked any evidence of respondent's contrition or lack of remorse for his conduct. His counsel asserted, however, that

respondent had expressed sincere remorse during their personal communications.

Following a de novo review of the record, we find there is clear and convincing evidence that respondent violated RPC 8.1(a) (two instances), RPC 8.4(b); and RPC 8.4(c) (three instances). We determine to dismiss the additional charged instance of RPC 8.1(a), which the DEC also rejected.

Specifically, we find the undisputed evidence clearly and convincingly establishes that respondent violated RPC 8.1(a) in two respects.[13] First, respondent violated that Rule by admittedly misrepresenting to the OAE, in his March 23, 2020 letter, that he had not intentionally accessed the Firm's computer system following his separation. Respondent subsequently confessed that he repeatedly and intentionally had accessed the Firm's system, knowing that he was unauthorized to do so.

We determine that respondent separately violated RPC 8.1(a), contrary to the DEC's finding, by denying having installed TeamViewer on his former Firm desktop computer. Bratton unambiguously testified that the Firm did not use TeamViewer and that he would not have authorized its installation. Minker

[13] We agree with the DEC's conclusion that the evidence surrounding respondent's separation from the Firm was not settled to the standard of clear and convincing evidence. R. 1:20-6(c)(2)(B). We, thus, decline to find a third violation of RPC 8.1(a) on the theory that respondent knowingly misrepresented to the OAE that he had not been terminated from the Firm.

corroborated Bratton's testimony on behalf of the Firm's information technology company. Minker testified that Able Technology had not installed TeamViewer on any Firm office computer, including the desktop previously assigned to respondent. Further, Bravette, who had witnessed respondent's covert remote activity, testified that the name "Justin Scott" appeared on the computer screen while respondent was remotely accessing Bratton's computer system. Bravette also testified that he did not use TeamViewer and was unaware of its installation on his desktop until the night he observed respondent's remote activity. Moreover, respondent admittedly used TeamViewer while employed by, and following his separation from, the Firm. Thus, despite his denial, the overwhelming circumstantial evidence clearly and convincingly establishes that respondent installed TeamViewer on his former office desktop and, therefore, further violated RPC 8.1(a) by denying this fact to the OAE.

Respondent's misrepresentations to the OAE in these respects, namely that he had neither installed TeamViewer, nor accessed the Firm's computer system following his separation from the Firm, also violated RPC 8.4(c), which prohibits an attorney from engaging in conduct involving dishonesty, fraud, deceit or misrepresentation.

Next, respondent admittedly violated RPC 8.4(b), which prohibits a lawyer from committing "a criminal act that reflects adversely on a lawyer's

honesty, trustworthiness or fitness as a lawyer in other respects." It is well-settled that a violation of this Rule may be found even in the absence of a criminal conviction or guilty plea. See In re Gallo, 178 N.J. 115, 121 (2003) (the scope of disciplinary review is not restricted, even though the attorney was neither charged with nor convicted of a crime); In re McEnroe, 172 N.J. 324 (2002) (attorney found to have violated RPC 8.4(b), despite not having been charged with or found guilty of a criminal offense). Respondent's unlawful and unauthorized access to the Firm's computer system constituted a third-degree crime, contrary to N.J.S.A. 2C:20-25(a) and (e).[14]

N.J.S.A. 2C:20-25, governing computer crimes, provides, in relevant part:

> A person is guilty of computer criminal activity if the person purposely or knowingly and without authorization, or in excess of authorization:
>
> a. Accesses any data, data base, computer storage medium, computer program, computer software, computer equipment, computer, computer system or computer network;
>
> . . .
>
> e. Obtains, takes, copies or uses any data, data base, computer program, computer software, personal

[14] N.J.S.A. 2C:20-25(g) provides that a violation of subsection (a) or (e) constitutes a crime of the third degree, except that a violation of subsection (e) constitutes a crime of the second degree if the information contains "(1) personal identifying information, medical diagnoses, treatments or other medical information concerning an identifiable person; (2) is or contains governmental records or other information that is protected from disclosure by law, court order or rule of court; or (3) has a value exceeding $5,000."

> identifying information, or other information stored in a computer, computer network, computer system, computer equipment or computer storage medium[.]

Consistent with that plain language, the conduct must be "knowing." N.J.S.A. 2C:2-2b(2) ("[a] person acts knowingly with respect to the nature of his conduct or the attendant circumstances if he is aware that his conduct is of that nature, or that such circumstances exist, or he is aware of a high probability of their existence. A person acts knowingly with respect to a result if he is aware that it is practically certain that his conduct will cause such a result").

Here, respondent stipulated that, on at least six occasions, he intentionally accessed the Firm's computer system, despite knowing that he was unauthorized to do so. Further, respondent admitted that, by doing so, he had obtained, at a minimum, confidential information regarding Bratton's calendar, clients, and timekeeping activities. Thus, he violated RPC 8.4(b).

Further, by repeatedly and surreptitiously accessing his former law firm's computer system following his separation from the Firm, respondent again violated RPC 8.4(c). Respondent knew he was not permitted to access that system but did so anyway to, at a minimum, quench his curiosity concerning the status and success of Bratton's legal practice.

In sum, we find that respondent violated RPC 8.1(a) (two instances); RPC 8.4(b); and RPC 8.4(c) (three instances). The sole issue remaining for our

determination is the appropriate quantum of discipline for respondent's misconduct.

Generally, in matters involving misrepresentations to ethics authorities, the discipline ranges from a reprimand to a term of suspension, depending on the gravity of the offense, the presence of other unethical conduct, and aggravating or mitigating factors. See, e.g., In re DeSeno, 205 N.J. 91 (2011) (reprimand for an attorney who misrepresented to the district ethics committee the filing date of a complaint on the client's behalf; the attorney also failed to adequately communicate with the client and failed to cooperate with the investigation of the grievance; prior reprimand); In re Otlowski, 220 N.J. 217 (2015) (censure for an attorney who made misrepresentations to the OAE and to the client's lender by claiming that funds belonging to the lender, which had been deposited into the attorney's trust account, were frozen by a court order; to the contrary, the funds had been disbursed to various parties; violations of RPC 8.1(a) and RPC 8.4(c) found; no prior discipline); In re Freeman, 235 N.J. 90 (2018) (three-month suspension for pool attorney with the Office of the Public Defender (OPD); the attorney failed to communicate with his client about an upcoming hearing on a petition for post-conviction relief; the attorney appeared at the hearing without the client, took actions that were contrary to the client's wishes, and made misrepresentations to the court and to the OPD; those

statements would later negatively impact the client's ability to pursue an appeal; during the ethics investigation, the attorney lied to the DEC investigator and, later, to the hearing panel; violations of RPC 1.2(a) (failing to abide by the client's decisions), RPC 1.4(b) (failing to keep a client reasonably informed about the status of the matter), RPC 3.3(a) (making a false statement of material fact to a tribunal), RPC 4.1(a) (making a false statement of material fact or law to a third person), RPC 8.1(a), and RPC 8.4(c) found; no prior discipline); In re Silberberg, 144 N.J. 215 (1996) (two-year suspension imposed on attorney who, in a real estate closing, allowed the buyer to sign the name of the co-borrower; the attorney then witnessed and notarized the "signature" of the co-borrower; the attorney stipulated that he knew at the time that the co-borrower was deceased; after the filing of the ethics grievance against him, the attorney falsely stated that the co-borrower had attended the closing; on another occasion, the attorney sent a false seven-page certification to the district ethics committee in order to cover up his improprieties; violations of RPC 8.1(b), RPC 8.4(b), and RPC 8.4(c) found); In re Penn, 172 N.J. 38 (2002) (three-year suspension for attorney who failed to file an answer in a foreclosure action, thereby causing the entry of default against the client; thereafter, to placate the client, the attorney lied that the case had been successfully concluded, fabricated a court order, and

signed the name of a judge; the attorney then lied to his adversary and to ethics officials; the attorney also practiced law while ineligible).

Thus, for respondent's misrepresentations to the OAE, standing alone, a reprimand is the appropriate quantum of discipline. Respondent, however, committed additional, serious misconduct.

For respondent's violations of RPC 8.4(b) and RPC 8.4(c), in connection with his repeated, unauthorized entries into the Firm's computer system, our decision in In re Alper, 242 N.J. 143 (2020), provides relevant guidance. In Alper, the Court imposed a reprimand for an attorney's illegal and unauthorized access to his former employer's subscription database, in violation of RPC 8.4(b) and RPC 8.4(c). In that matter, Alper had been employed as the Director of Operations by Marine Transport Logistics (MTL), a shipping company owned by his parents-in-law. In the Matter of Vadim Alper, DRB 19-194 (January 14, 2020) at 2. Alper's position required little legal work so his role with MTL changed, requiring him to travel internationally, soliciting clients, for which he was compensated via a one-third commission on all profits that he generated. Ibid.

After a falling out, Alper's in-laws stopped paying his earned commissions. Ibid. Alper subsequently formed a competitor company and left MTL. Alper admitted that, after leaving MTL, he had, on several occasions,

improperly used the login credentials belonging to existing MTL employees, which credentials he had created while working at MTL (because his own credentials had been revoked), to access a subscription-based database of shipping information. Alper contended that he had accessed the database solely for the purpose of calculating the commissions he was owed, for use in connection with his ongoing civil litigation against MTL.

Alper was charged with second and third-degree computer criminal activity, in violation of N.J.S.A. 2C:20-25(c) and (e), and, following the downgrade of the second-degree charge, was admitted into pretrial intervention for a twelve-month term. Alper admitted that his actions were illegal and violative of RPC 8.4(b) and (c). To determine the appropriate quantum of discipline, we examined two lines of disciplinary precedent involving closely analogous criminal conduct, namely thefts by attorneys and conduct involving less serious criminal acts, because there was no precedent directly on point.

We acknowledged that theft by an attorney generally results in a term of suspension, the length of which depends on the severity of the crime and the presence of mitigating or aggravating factors. Id. at 6. We determined, however, that the unique circumstances of respondent's computer crimes were not as egregious as the circumstances underpinning other attorney theft cases and, thus, did not necessitate a term of suspension.

Rather, we viewed Alper's computer criminal actively as analogous to that of attorneys who had engaged in less serious criminal acts and were admonished or reprimanded for their misconduct. See, e.g., In the Matter of Michael E. Wilbert, DRB 08-308 (February 11, 2009) (admonition for possession of eight rounds of hollow-point bullet ammunition and possession of an over-capacity ammunition magazine, fourth-degree crimes for which the attorney was admitted into pre-trial intervention); In re Murphy, 188 N.J. 584 (2006) (reprimand imposed on attorney who twice presented his brother's driver's license to police in order to avoid prosecution for driving-under-the-influence charges, in violation of RPC 8.4(b), RPC 8.4(c), and RPC 8.4(d); in addition, the attorney failed to cooperate with the OAE's investigation of the matter, in violation of RPC 8.1(b)); In re LaVergne, 168 N.J. 409 (2001) (reprimand for attorney found guilty in municipal court of theft by failure to make required disposition of property received, a disorderly persons offense; the attorney entered into an agreement to purchase an automobile, never made payment, and instead took possession of the vehicle and allowed it to be registered to a new owner).

Based upon the foregoing precedent, we determined to reprimand Alper, and the Court agreed. Although Alper had no prior discipline in his years at the bar, and had stipulated to his misconduct, we determined that a reprimand was

appropriate in view of his covert and repeated unauthorized access to the database, using login credentials that were not his own. Ibid.

Here, like the attorney in Alper, respondent knowingly and repeatedly accessed a former employer's computer system to which his access had been revoked. Unlike Alper, however, who freely admitted to his misconduct, respondent initially denied responsibility and made misrepresentations to the OAE regarding (1) his state of mind while accessing the Firm's computer system, and (2) the fact he had installed the software that provided him with the unauthorized access. Moreover, Alper received a reprimand, in part, because we weighed, in mitigation, that he had fully cooperated by having stipulated to his misconduct, a fact not present here.

Here, based upon our reasoning in Alper, the totality of respondent's misconduct warrants more severe discipline than the reprimand imposed in that matter. Thus, consistent with the OAE's and the DEC's recommended quantum of discipline, we conclude that a censure is the baseline discipline for the totality of respondent's misconduct. However, to craft the appropriate discipline, we further consider both mitigating and aggravating factors.

In mitigation, this is respondent's first brush with the disciplinary system in his eight years at the bar. In re Convery, 166 N.J. 298 (2001). However, given his short career at the time of his misconduct, we accord this factor minimal

weight. Likewise, as the DEC correctly observed, we assign no weight to respondent's alleged "exemplary conduct" since his violations underlying this matter. Respondent is obligated, as an attorney in New Jersey, to adhere to the Rules of Professional Conduct. See, e.g., In re Hasbrouck, 140 N.J. 162, 167 (1995) (attorneys are obligated to adhere to the high standard of conduct required by members of the bar).

In aggravation, respondent demonstrated a lack of remorse for his misconduct, evidenced, in part, by his evolving explanations for his unauthorized access to Bratton's computer database and his continued denial that he had installed the TeamViewer program on his former office desktop. Regardless of whether he was motivated by his competitiveness with Bratton, or some other nefarious or self-serving purpose, the fact remains that respondent surreptitiously gained access to a secure database that contained confidential client information, to which he was not privy. This type of misconduct has the potential to undermine the public's confidence in the bar and, accordingly, we seek to deter such behavior in the future.

On balance, and consistent with disciplinary precedent, we determine that a censure is the appropriate quantum of discipline necessary to protect the public and preserve confidence in the bar.

Chair Gallipoli voted to impose a three-month suspension.

Member Joseph was absent.

We further determine to require respondent to reimburse the Disciplinary Oversight Committee for administrative costs and actual expenses incurred in the prosecution of this matter, as provided in R. 1:20-17.

Disciplinary Review Board
Hon. Maurice J. Gallipoli, A.J.S.C. (Ret.),
Chair

/s/ Timothy M. Ellis

By: _____
Timothy M. Ellis
Acting Chief Counsel

SUPREME COURT OF NEW JERSEY
DISCIPLINARY REVIEW BOARD
VOTING RECORD

In the Matter of Justin L. Scott
Docket No. DRB 22-066

Argued: September 15, 2022

Decided: October 27, 2022

Disposition: Censure

Members	Censure	Three-Month Suspension	Absent
Gallipoli		X	
Boyer	X		
Campelo	X		
Hoberman	X		
Joseph			X
Menaker	X		
Petrou	X		
Rivera	X		
Singer	X		
Total:	7	1	1

/s/ Timothy M. Ellis

Timothy M. Ellis
Acting Chief Counsel