

BEFORE THE  
CALIFORNIA BOARD OF ACCOUNTANCY  
DEPARTMENT OF CONSUMER AFFAIRS  
STATE OF CALIFORNIA

In the Matter of the Citation Against:

NED ALAN LEIBA  
Stockton, California 95202

Certified Public Accountant  
Certificate No. CPA 23912

Respondent.

Case No. CT-2016-1

OAH No. 2015090140

**PROPOSED DECISION**

The above-entitled matter was heard by Stephen J. Smith, Administrative Law Judge (ALJ), Office of Administrative Hearings (OAH), State of California, on January 4, 2016, in Sacramento, California.

Stanton Lee, Deputy Attorney General, Department of Justice, State of California, represented the California Board of Accountancy (CBA), Department of Consumer Affairs, State of California.

Respondent Ned Alan Leiba, C.P.A., appeared and represented himself.

Evidence was presented, the matter was argued and was submitted for Decision on January 4, 2016.

**ISSUES**

1. Was respondent's refusal to obtain and submit a new set of Live Scan fingerprints from the California Department of Justice, Criminal Records and Identification section (CA DOJ CII), directed to the CBA in conjunction with his application to renew his Certified Public Accountant (CPA) license in active status for the renewal period ending September 30, 2014, a violation of California Code of Regulations, title 16, section 37.5 (section 37.5), or was his refusal justified?

2. Does respondent comply with the requirements of section 37.5, subdivision (a), because he submitted a full paper set of his rolled fingerprints to the CBA as part of his initial licensure in 1976?

3. What is the legal effect of the CBA's destruction of respondent's fingerprints submitted to the CBA in 1976, and the destruction of its records of respondent's submission?

4. Can the CBA obtain a Criminal Offender Record Information (CORI) state and federal criminal record clearance report for respondent from the CA DOJ CII without respondent's submission of a new set of Live Scan electronic fingerprints to the CBA through the CA DOJ CII?

5. Can the CBA obtain a CORI from the CA DOJ CII for respondent through respondent providing written authorization to the CBA, permitting access to his digital fingerprints on file with the U.S. Department of Homeland Security (US DHS) the U.S. Department of Justice (US DOJ) or the Federal Bureau of Investigation (FBI) or other law enforcement data base?

6. If respondent violated the regulation, and his conduct was not justified, was the CBA's imposition of a \$500 administrative penalty appropriate and reasonable under the circumstances?

## CONTENTIONS

### CBA'S CONTENTIONS

1. The CBA contends respondent violated section 37.5, because he unjustifiably failed, despite notice and warnings, to obtain and submit a new set of Live Scan electronic fingerprints to the CBA, through the CA DOJ CII. The CBA contends respondent's previous submission of his paper rolled fingerprints do not satisfy the requirements of section 37.5.

2. The CBA contends that section 37.5 requires that respondent submit a new Live Scan set of digital fingerprints to the CBA through the CA DOJ CII, because he has no fingerprints on file with, or available to, the CBA. The Board contends that, "[E]ven if the licensee completed the fingerprint process as a condition for licensure, if no electronic record of the licensee's fingerprints exists with the DOJ, the licensee must still submit the fingerprints as a condition of renewal"<sup>1</sup>

3. The CBA contends that if respondent is not required by section 37.5 to submit a new set of electronic fingerprints via Live Scan, the CBA will have no other access to respondent's fingerprints, because the CBA does not have any fingerprints for respondent on file, and respondent's fingerprints submitted to the CBA as part of his original licensure were destroyed. The CBA contends that respondent's fingerprints are essential to identify him and for the CA DOJ CII to use those fingerprints to search its records and produce a CORI<sup>2</sup> state

---

<sup>1</sup> CBA Enforcement Chief's letter to respondent, dated March 30, 2015, Exhibit 5, Bates AG0228.

<sup>2</sup> CORI is an acronym for a Criminal Offender Record Information. A CORI is a criminal records clearance and information report produced by the CA DOJ CII upon request

and federal criminal records clearance, which the CBA is required to obtain and review for every licensee. The CBA thus contends that unless respondent submits new Live Scan fingerprints, it has no other way to perform its statutory duty, and that section 37.5 was enacted to make certain every new or renewing licensee produces his or her fingerprints to the CBA for the purpose of fulfilling this duty.

4. The CBA contends it has no other access to respondent's fingerprints or his state and federal criminal records that might exist elsewhere and cannot obtain a clearance for him without respondent submitting new fingerprints to the CBA as required by section 37.5. The CBA contends Penal Code section 11142 prohibits access by the CBA to respondent's fingerprints that may be on file for him at the CA DOJ CII or that exist in any other law-enforcement database, because his fingerprints, even if in electronic form and recently obtained exist, cannot be accessed by the CBA because it was provided by a "third party" source, other than by a CBA submission of respondent's fingerprints and request for a CORI. CBA contends it is a misdemeanor to have respondent's fingerprint information disclosed to, or received by, the CBA, that may exist and be provided by any source other than a CBA request. The CBA contends respondent's authorization for access to any digital fingerprints respondent may have on file with the CA DOJ CII or any other law-enforcement database is ineffective due to Penal Code section 11142.

5. The CBA contends the penalty it selected in the Citation was reasonable considering the circumstances.

#### RESPONDENT'S CONTENTIONS

6. Respondent contends that he complied with section 37.5, subdivision (a), because he submitted a full set of rolled paper fingerprints to the CBA as part of his original licensure in 1976. Respondent contends that his submission of his rolled fingerprints as part of his original licensure as a CPA complied with section 37.5, subdivision (a), which he contends provides an alternative for compliance besides submission of a new set of Live Scan digital fingerprints. Respondent contends that the CBA retained copies of his fingerprints after he submitted them in 1976, that the CBA provided his fingerprints to the CA DOJ CII as part of obtaining a CORI state and federal criminal record clearance report

---

of an applicant for a license or renewal, a sensitive job, a permit requiring a clearance, and so forth, for an individual, agency or entity authorized to request/receive such a report. The CA DOJ CII uses an individual's fingerprints to identify that person and produces the CORI after reviewing criminal history and records of the person about whom the report is requested, and then reports whether that person does or does not have a criminal history, and, if so, what criminal records exist. The CBA requires fingerprint records from all licensees so that it can report that information to the CA DOJ CII and request a search of its licensees and obtain CORI report on each with a record, to make certain the licensee does not have a criminal record, or to report on whether that licensee suffered any criminal history activity during that licensee's renewal. Fingerprints must be submitted to the CA DOJ CII, already on file or accessible to the CA DOJ CII from some other authorized source, for the CA DOJ CII to research criminal records and generate a CORI clearance report to a requestor.

for him, as required by law, and was never advised otherwise until this action. He contends the CBA's demand he obtain a new set of Live Scan fingerprints with his most recent renewal application, when he already submitted his fingerprints to the CBA, and the CBA had or should have had access to his fingerprints, is unreasonable under the circumstances.

7. Respondent contends the CBA is construing section 37.5, subdivision (a) impermissibly narrowly, in a fashion that unreasonably excludes compliance by older licensees, such as him, who furnished fingerprints to the CBA in paper form years ago as a mandatory part of initial licensure.

8. Respondent contends that the CBA should not be able to penalize him for its own action reversing his compliance with section 37.5, subdivision (a) without notice to him. Respondent contends that absent the CBA's destruction of his fingerprints without notice of that action, he would be in compliance with section 37.5, subdivision (a), because he is a person who previously submitted his fingerprints as a condition of licensure. He contends that if he is required to obtain yet another Live Scan because the CBA destroyed his fingerprints, and thus his compliance with section 37.5, or is unwilling to access, with his authorization, the electronic fingerprints on file with the US DHS, the CBA should reimburse him for the additional cost as a matter of fairness.

9. Respondent contends that there are reasonable alternatives to the CBA demanding he submit a new set of Live Scan fingerprints, because access to his fingerprints and criminal records in order to produce a CORI state and federal criminal records clearance is reasonably available, and he is willing to authorize access to his records in writing. Respondent contends the CBA's claim that Penal Code section 11142 prohibits the CBA from access to his fingerprint records on file with the CA DOJ CII, received for purposes other than CBA licensure or renewal, or in federal law enforcement data bases, is not legally correct.

10. Respondent contends the CBA failed to prove they have no reasonable alternative to his providing new electronic fingerprints. Respondent contends the CBA failed to prove the CBA cannot obtain a CORI federal and state criminal record clearance report for him through the CA DOJ CII by use of his fingerprints already on file with the US DHS, US DOJ and/or the FBI via the US DHS. He contends he submitted a full set Live Scan digitized fingerprints in January 2013 to an official of the U.S. Customs and Boarder Protection, a division of the US DHS, as part of his approval as a Global Entry Trusted Traveler. Respondent contends the comprehensive state, federal and international criminal background check conducted by the Global Entry Trusted Traveler program used his Live Scan electronic fingerprints to identify him through the CA DOJ CII, US DHS, US DOJ, FBI and Interpol data bases and to produce a criminal records clearance for him even broader in scope than a CORI, after he submitted his electronic fingerprints in January 2013.

11. Respondent contends his electronic fingerprints are available to the CA DOJ CII and the CBA upon request for reasonable licensing criminal background checking, and that the CBA failed to prove otherwise. Respondent contends the CBA provided no evidence of any reason why the CBA did not or could not request access to his electronic fingerprints

in these federal data bases directly for its legally legitimate licensing criminal records background check, or through the CA DOJ CIL, through his repeatedly offered written authorization for the CBA to access his records.

12. Respondent contends that regardless of whether he is found in violation of the regulation, his actions were in utmost good faith, he reasonably believed submission of his fingerprints to the CBA in 1976 fully complied with the first alternative provided in section 37.5, subdivision (a), and he sought this hearing to contest what he contends is an unnecessarily narrow interpretation of the regulation, for the benefit of himself and other older licensees. Respondent contends his good faith and desire to be fully in compliance with all reasonable requests of the CBA to verify and research his federal and state criminal background to make sure he is crime free is evident in his repeated offers to provide written authorization to his existing fingerprints and criminal records, and to submit to a new and, what he contends is redundant, Live Scan within 30 days of the final disposition of his challenge here, should his interpretation be found in error. He contends that assessment of an administrative penalty for his challenge to what he contends is an unnecessarily restrictive interpretation of the regulation, and the exercise of his rights to seek review and a judicial determination of the appropriate construction of the regulation, for the benefit of himself and those similarly situated, is unreasonable and improperly punitive.

#### STANDARD AND BURDEN OF PROOF

The standard of proof to be applied is a preponderance of the evidence.<sup>3</sup> Preponderance of the evidence is that state of the evidence that makes proof of any fact or issue in dispute more likely than not.<sup>4</sup> The CBA bears the burden of proof and the burden of going forward with the evidence.

#### RESOLUTION OF CONTENTIONS

13. The CBA failed to prove that respondent violated section 37.5, subdivision (a). The CBA failed to prove that respondent does not satisfy the requirements of section 37.5, subdivision (a), which excludes from the requirement to submit new electronic fingerprints as a condition of licensure or renewal those who have previously provided fingerprints to the CBA in any form, paper rolled on cards or electronic, as part of their licensure. Respondent has previously provided his fingerprints to the CBA, and he proved his fingerprints were submitted in paper form to the CBA in 1976. Respondent proved he is a person who meets the requirements of subdivision 37.5, subdivision (a) because he was a not a "licensee applying for renewal as a CPA or Public Accountant who has not previously submitted fingerprints as a condition of licensure," thereby proving he is not subject to the remainder of the regulation requiring new licensees and other renewal applicants to submit a new Live Scan set of fingerprints.

---

<sup>3</sup> Business and Professions Code section 494, subdivision (c).

<sup>4</sup> Evidence Code section 115.

14. The CBA's action to destroy respondent's previously submitted fingerprints, and its records of those fingerprints, did not prevent respondent from being in compliance with section 37.5, subdivision (a). The CBA's unilateral and unnoticed action destroying respondent's fingerprints does not reverse the fact that respondent complied with the requirement by previously submitting his fingerprints. The CBA is equitably estopped from punishing respondent for the effects of its own action that reversed the manner in which respondent previously complied with its regulation. Respondent had no notice of the CBA's decision to destroy his fingerprints and its records of his submission, had nothing to do with it, and has been prejudiced by it through this enforcement action. Respondent proved his paper rolled fingerprints remained on file and available for use for identification and cross matching against his criminal history at CA DOJ CII and CBA licensure records, from 1976 until CBA destroyed those fingerprints its records of his submission on an unknown date.

15. The CBA failed to prove by a preponderance of the evidence that respondent's refusal to submit to a new Live Scan deprives the CBA of a reasonable alternative to obtain a copy of respondent's electronic fingerprints, besides compelling respondent to obtain a new Live Scan and seeking to punish him for his failure to do so. The CBA failed to prove that through CA DOJ CII does not have, or have reasonable access to, a digital record of respondent's fingerprints. The CBA failed to prove by a preponderance of the evidence that the CBA, through the CA DOJ CII cannot access, through respondent's written authorization, copies of respondent's digital fingerprints on file at either the CA DOJ CII, or on file with federal law enforcement agencies, such as US DHS, US DOJ or the FBI, and that those electronic fingerprints cannot be used to produce a CORI state and federal criminal records clearance on respondent. Business and Professions Code section 144.5 permits the CBA, an agency specifically identified in Business and Professions code section 144, access and the ability to lawfully receive, upon request, "from local or state agencies certified records of all arrests and convictions, certified records regarding probation, and any and all other related documentation needed to complete an applicant or licensee investigation." This authority does not require respondent's authorization to access or receive his records.

#### FACTUAL FINDINGS

1. Patti Bowers, acting in her official capacity only as Executive Officer (EO) of the CBA, issued Citation Order CT-2016-1 (Citation) to respondent on June 26, 2015. The CBA has the authority to regulate the practice of public accounting and to impose rules and standards governing the practice of accountancy in the State of California.<sup>5</sup> The CBA has the authority to impose disciplinary action upon any holder of a license to practice as a certified public accountant in the State of California for violation of those rules and standards.<sup>6</sup>

---

<sup>5</sup> Business and Professions Code sections 5018 and 5019. All further statutory references are to sections of the Business and Professions Code.

<sup>6</sup> Section 5050.2.

2. Respondent timely sought an evidentiary hearing on the Citation. Respondent's appeal of the Citation was set to be heard by an ALJ of the OAH.<sup>7</sup>

3. The Citation alleges a single violation of section 37.5 and seeks an administrative fine of \$500. The Citation alleges that respondent "failed to complete a state and federal level criminal offender record information search by submitting fingerprints prior to renewing his license in active status for the renewal period that ended September 30, 2014." The Citation orders respondent to "complete a criminal offender record information search conducted by the Department of Justice," and to pay the administrative fine.

4. The Citation does not fully or accurately describe the noncompliance problem the CBA seeks to enforce against respondent. Respondent cannot obtain, complete or submit a CORI himself, as the Citation allegation suggests. The CBA faults respondent in the Citation for failure to obtain and submit to the CBA a new Live Scan electronic set of fingerprints, from which respondent can be identified, and a CORI produced by the CA DOJ CII, using that identifying information.

5. The CBA issued respondent CPA certificate number 23912 on December 10, 1976. The CBA renewed respondent's license every other year from issuance through September 30, 2014. The CBA granted respondent's renewal application for the period September 30, 2014 through September 30, 2016, but later raised the matter at issue in the Citation. The CBA has no record of disciplinary action against respondent in the 40 years he has been licensed as a CPA.

6. Respondent submitted a full set of rolled paper fingerprints to the CBA as part of his initial licensure in 1976. Respondent believed that the CBA submitted a copy of his fingerprints to the CA DOJ CII, and that the CBA and the CA DOJ CII retained his paper fingerprints in their records. Respondent's first notice that the CBA did not still have a copy of his rolled paper fingerprints or records of his submission of his fingerprints as a part of his licensure did not occur until 2015.

7. Respondent's application for renewal for the period September 30, 2014 through September 30, 2016, did not contain, nor was it augmented by, his submission of a new set of Live Scan fingerprints to the CBA. Respondent's application for his most recent license renewal contained the same information that he had provided in each of his previous 19 consecutive bi-annual renewals, including his declaration under penalty of perjury that he had not been convicted of any criminal offense during the most recent renewal period.

8. The CBA advised respondent in writing on January 27, 2015, that his application renewal was deficient because the CBA had, "not received a record of your fingerprint submission, as set forth in CBA regulation section 37.5." The CBA further advised:

---

<sup>7</sup> Section 125.9, and Government Code section 11550, et. seq.

In order to comply with section 37.5, you must submit fingerprints within 30 days from the date of this letter. Upon successfully completing the submission of fingerprints, please provide the CBA a copy of your completed *Request for Live Scan Service* form so that we may work with the California Department of Justice (DOJ) to obtain your fingerprint record. The *Request for Live Scan Service* form and instructions are enclosed for your reference. If you previously submitted fingerprints for the CBA via the live scan process and have a copy of your completed *Request for Live Scan Service* form, please submit the copy to the CBA so that we may request your Criminal Offender Record Information (CORI) clearance from the DOJ. (Italics in original.)

9. Respondent replied in writing to the CBA on January 30, 2015. Respondent wrote that he called the CBA's CORI Unit phone number posted on the CBA's website immediately upon receipt of the CBA's January 27, 2015 letter, and spoke to CBA representative "Lonnie."<sup>8</sup> Respondent noted that Lani, "confirmed that my fingerprints were recorded and received by the CBA in 1976." Respondent claimed that he satisfied the requirements of section 37.5, because his fingerprints, on file with the CBA since 1976, met the requirements of Section 37.5, that provides ... "or for those who did not use an electronic fingerprint system, a receipt evidencing that his or her fingerprints were recorded and submitted to the CBA." He requested copies of the documents reviewed by Lani during his January conversation with her that showed that he submitted and the CBA received his fingerprints in 1976.

10. The CBA's Enforcement Chief (EC) replied in writing on February 17, 2015. He wrote first regarding respondent's request for confirmation that his previously submitted fingerprints from 1976 satisfied the requirements of section 37.5:

At one point in time the CBA did collect fingerprints from examination candidates with the intention of having them processed for initial licensing. Subsequently, the CBA determined that this step would not be undertaken, and took the necessary steps to remove and destroy all fingerprint cards from the licensee's files. I apologize if there was some miscommunication regarding the CBA's historical records related to fingerprints.

11. There was no evidence of any official CBA action to destroy licensee fingerprints on file with the CBA that the CBA previously demanded be submitted by licensees as part of their licensure. There was no evidence of any official CBA authorization to take action to destroy licensee fingerprints or CBA records that licensees had submitted their fingerprints to the CBA. There was no evidence that the CBA put the matter of

---

<sup>8</sup> It appears "Lonnie" is CBA CORI Unit employee Lani Ascalon.



destroying licensee fingerprints on a CBA Board Meeting agenda, or gave licensees who had submitted fingerprints to the CBA any notice that it was contemplating such an action or provided such licensees an opportunity to comment or consider an alternative. There was no evidence when the licensee fingerprint records were destroyed, who gave the order to destroy them, who actually destroyed the records, or when the destruction was completed. There was no evidence that the CBA notified respondent that the CBA had decided to destroy his previously submitted fingerprints and not submit them to the CA DOJ CII. There was no evidence that the CBA provided respondent an option to pay the cost to have his fingerprints transmitted, processed and recorded by the CA DOJ CII, to be retained their records, or receive back his fingerprints, as an alternative to the CBA deciding to destroy those records without notice.

12. The CBA's EC also wrote in his February 15, 2015 letter:

When the CBA undertook the retroactive fingerprint program, it obtained a list from the California Department of Justice (DOJ) that included all CBA licensees with whom an electronic record of fingerprints exists. ***According to the DOJ, a record of your fingerprints does not exist.***<sup>9</sup> Therefore, in order to comply with CBA regulations section 37.5, you are required to submit electronic fingerprints to the DOJ via the live scan processes before your next renewal. (Emphasis added.)

13. Respondent replied in writing to the EC on February 25, 2015. Respondent advised that the CBA's letter of February 17, 2015 failed to address his specific concern because the CBA's representative Lani told him during their telephone conversation that she saw in the CBA's records that respondent's fingerprints were recorded as received by the CBA. Respondent requested copies of the fingerprint records that Lani discussed with him on the phone because he understood that Lani had reviewed and confirmed the existence of those records during their telephone conversation. Respondent also wrote:

As I also explained to Lonnie, my scanned fingerprints exist in the U.S. Customs and Border Protection database. Every time I enter the U.S., my fingerprints are electronically scanned and matched with those records. Accordingly, I have no objection to the proper use of my scanned fingerprints. I believe the CBA, as a policy to avoid duplicative effort and minimize costs, should determine if the Department of Justice can obtain scanned fingerprints from federal agencies.

---

<sup>9</sup> The EC clarified in his testimony that he did not mean there was no record at the DOJ at all of respondent's fingerprints, only that the DOJ did not have fingerprints specifically submitted by respondent for the CBA.

14. The CBA's EC replied in writing on March 30, 2015. He wrote:

As I noted, at one time the CBA did collect fingerprints from examination candidates with the intention of having them processed for initial licensure. Subsequently, the CBA determined that this step would not be undertaken, and took the necessary steps to remove and destroy all fingerprint cards from licensee's files. The fingerprint cards were not sent to the Department of Justice (DOJ) for the purpose of performing criminal offender record information<sup>10</sup> searches. ***While the CBA does recognize that certain applicants did submit the fingerprint cards, it does not maintain a record of submission. CBA does not have a record of your fingerprint submission.***<sup>11</sup> I apologize if there was a miscommunication regarding the records the CBA maintains historical records on fingerprints.

... Even if the licensee completed the fingerprint process as a condition for licensure, if no electronic record of the licensee's fingerprints exists with the DOJ, the licensee must still submit the fingerprints as a condition for license renewal. At this point is important to note that ***while an electronic record of your fingerprints may exist with the DOJ***, as indicated in your letter, ***this record is specific to the agency for which the fingerprints were submitted.*** Penal Code section 11142 makes it a misdemeanor to share fingerprint records....

... Based on the record submitted to the CBA from the DOJ, no electronic record of your fingerprints exists. (Emphasis added.)

15. The CBA's EC wrote respondent another letter, dated June 2, 2015, advising him that the CBA found him to be in violation of section 37.5. He advised respondent that as a result of the CBA's findings, a Citation and fine "may be issued" to him. The EC attached a page from the Adoption Rationale, supporting enactment and approval of section 37.5, to his June 2, 2015 letter. In the portion of the attachment entitled Factual Basis/Rationale, the following appears:

The purpose of the proposed regulatory changes is to ensure that the CBA upholds its mandate to protect the public in accordance with section 5000.1<sup>12</sup> in order to protect the public from

---

<sup>10</sup> CORI clearance report.

<sup>11</sup> It appears that the Board's destruction of licensee fingerprints encompassed not only the actual fingerprints, but any records that the licensee actually submitted them.

<sup>12</sup> All references are to the Business and Professions Code.

unethical and unprofessional practitioners. It is necessary for the CBA to be informed of past current criminal convictions that are substantially related to the qualifications, functions or duties of their profession for which they are licensed. ... In order to fully implement the CBA's authority to discipline a licensee that has been convicted of a crime substantially related to the qualifications, functions or duties of their profession, the CBA must receive all information related to those criminal convictions.

The fingerprinting requirement ensures an accurate criminal history record check is performed in order to best protect the public which is the CBA's highest priority. This proposal will extend the fingerprinting requirement to those who are already licensed, thus extending the protection of the public by ensuring that the CBA receives timely notification of any arrests or convictions concerning all of its licensees from the DOJ in the future.

[¶] ... [¶]

16. The Deputy Director for Communications (Deputy Director) of the DCA responded to a California Public Records Act (CPRA) request filed by respondent in June 2015. The Deputy Director advised respondent that the CBA's EO, "personally performed a diligent search of the files and records of the CBA for an electronic record of your fingerprints."<sup>13</sup> (Emphasis in original.) He also advised that the CBA's EO reviewed respondent's license file for information pertaining to his fulfillment of the fingerprint requirement as a condition of CBA licensure, and concluded that the records and files of the CBA contain no information that respondent has "satisfied the fingerprint requirement." The Deputy Director continued, "Since an electronic record of respondent's fingerprints does not exist" in the CA DOJ CII's CORI database<sup>14</sup>, respondent is in violation of the CBA regulation, unless he successfully submits new electronic fingerprints.

---

<sup>13</sup> Respondent's CPRA request was not limited to a request for any electronic records of his fingerprints contained in his CBA licensure records. Respondent never contended or suggested that he had electronic fingerprints on file with the CBA. Respondent sought records of his paper rolled fingerprints that were submitted to the CBA long before fingerprints could be captured digitally or stored electronically. Respondent sought from his first contact with the CBA's CORI Unit employee Lani Ascalon on January 29, 2015, confirmation that the CBA had records of his paper, rolled fingerprints he was required to submit to the CBA in 1976 as part of his initial licensure.

<sup>14</sup> No evidence was presented that would provide any foundation for this statement. No evidence was presented that anyone from the CBA or the DCA made a request of the CA DOJ CII to determine whether respondent had fingerprints, electronic or otherwise, on file with the CA DOJ CII, or whether a CORI could be produced for him using existing records.

17. Respondent wrote to the CBA on June 12, 2015, in response to the June 2, 2015 "Citation Pending Letter." Respondent expressed his willingness to undergo additional Live Scan fingerprinting, but with the understanding that he wanted to expeditiously appeal his case. Respondent reiterated that offer in his point by point appeal of the Citation on July 15, 2015, where he argued that if there is a determination that he must obtain additional fingerprints, he should be allowed 30 days from the date of the final determination to provide them. He restated his continuing offer to undergo additional fingerprinting again during his correspondence with the Deputy Attorney General, where he wrote in an email on December 15, 2015, that, "If there is a final determination that I need to have electronic fingerprints submitted to the CBA to be properly licensed as of September 2015, I will obtain the live scan fingerprints within 30 days of that determination."

#### ELECTRONIC FINGERPRINTS IN FEDERAL DATABASES

18. Respondent's digitized fingerprints have been on file with the US DHS, US Customs and Border Protection, Global Entry Trusted Traveler Program (Global Entry), since at least January 31, 2013. Respondent was required to submit documentation in person that he met the requirements for Global Entry after September 27, 2012, when his application to become a Trusted Traveler was acknowledged. Respondent submitted to a Live Scan and provided the US DHS a full set of scanned electronic fingerprints through officers of the US Customs and Border Protection, Global Entry, a division of the US DHS, at San Francisco International Airport. Respondent was told his electronic fingerprints were necessary in order to conduct a mandatory comprehensive state, federal and international background and criminal record check to verify that he had been crime free, a requirement to become a Trusted Traveler and pass through international borders and in and out of the US with minimal to no screening.<sup>15</sup> Respondent also understood that he was giving approval to permit his electronic fingerprints to be submitted to CA DOJ CII, US DOJ, the FBI and Interpol, to be used to identify him against records in those law enforcement databases as part of the screening process. Respondent received his criminal record clearance by the US DHS, after the state, federal and international criminal record background check, as evidenced by being granted Global Entry approval As a Trusted Traveler on January 31, 2013.

19. Respondent testified that when he travels internationally and reenters the United States, which he has done several times in the most recent few years and during the period of the pendency of this renewal, his fingerprints on file with the US DHS are digitally scanned and accessed by U.S. Customs and Immigration Officers through their electronic identification system. Respondent testified that in each instance, his electronic fingerprints he submitted to the US DHS with his application for Global Entry have been successfully accessed in the federal identification database, and he has always been permitted reentry.

---

<sup>15</sup> <http://www.cbp.gov/travel/trusted-traveler-programs/global-entry/eligibility>, accessed January 22, 2016 and January 26, 2016, Exhibit T, that lists requirements for approval.

20. Respondent has repeatedly offered to authorize in writing to provide the CBA access to his electronic fingerprints on file with the US DHS, as a reasonable alternative to being required to obtain, pay for and submit a new Live Scan to the CBA. Respondent's offer has been repeatedly refused.

21. The CBA's October 1, 2000, official newsletter to licensees included an article entitled, "New Fingerprinting Technology Available to Licensure Applicants." The CBA advised licensees in this article that:

The Accountancy Act requires all candidates applying for the California CPA license to submit fingerprint cards for the purpose of conducting a criminal history check with the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI). In the past, it took up to four months to process fingerprint cards, making the process of obtaining the initial license much longer. Now, there is a quicker way-an alternative to the rolling process that uses ink and 8" x 8" fingerprint cards. Live Scan is inkless, electronic fingerprinting by which the prints are electronically submitted to the DOJ. Digitizing the fingerprints enables the automatic transfer of fingerprint image data in combination with personal information to the DOJ computers in a matter of seconds....

The CBA continues to accept "manual" applicant fingerprint cards which are analyzed by a qualified technician trained and fingerprint techniques. Applicants who pass the CPA exam automatically received a CPA licensure packet with two fingerprint cards.<sup>16</sup> In addition, the fingerprint packet request form (request for both fingerprint cards and live scan service, is available at the CBA office and also on the CBA website.... Applicants living outside California must continue to use the fingerprint cards unless Live Scan is available in their states.

22. The CBA's Final Statement of Reasons (CBA's Final Statement) supporting the adoption of section 37.5, January 27, 2012, contained a section for "Comments, Objections or Recommendation/Responses." The CBA's Final Statement recited several questions by a Mr. Gai regarding the applicability of section 37.5. The CBA wrote regarding Mr. Gai's comments:

---

<sup>16</sup> No evidence was presented that contradicted respondent's contention that this is exactly what happened with his initial licensure, and how his fingerprints came to be submitted and on file with the CBA in 1976. Respondent had his fingerprints rolled upon the cards provided to him by the CBA, and submitted them to the CBA for a criminal record background check that was favorably concluded before the CBA issued him his license.

Due to the fact that the language is clear that a licensee applying for renewal must submit fingerprints in two cases;

1. When the licensee has not previously submitted fingerprints as a condition of licensure, or
2. When an electronic record of the licensee's fingerprints does not exist in the Department of Justice's criminal offender record identification database.

23. The CBA's Final Statement also responded to a question by an attorney, Mr. Bret, who submitted his question in an appended email, dated March 13, 2012. The CBA's Final Statement responded to Mr. Bret's inquiry seeking confirmation that a CPA licensee who became a Notary Public in 2011, and submitted electronic scanned fingerprints to the CA DOJ for a criminal background check as a part of the Notary application for a Commission from the California Secretary of State, would not have to submit another set of fingerprints at the time of CPA license renewal after 12/31/13 because that CPA licensee is not a person, "for whom an electronic record of the licensee's fingerprints does not exist in the Department of Justice's criminal offender record identification database." The CBA's Final Statement answered Mr. Bret's question by rejecting it, because, "Third parties are not allowed to share confidential fingerprint information, so the CBA would not have access to fingerprints collected for other purposes (Penal Code sections 11105, subdivision (b) (10), 11142, 11143)."

#### TESTIMONY

24. The CBA's EC was the only witness summoned by the CBA. His testimony consisted largely of statements that lacked foundation, and were thus unpersuasive, hearsay or opinion, with the exception of his reference to his correspondence with respondent and the CBA described above. The EC claimed, for example, that there is no electronic record of respondent's fingerprints on file with the CA DOJ CII available to the CBA. He failed to produce any document or supporting record from the CA DOJ CII to provide foundation for that claim. The EC and/or the EO did not request, obtain or produce a Penal Code section 11124 Declaration of Non-Existence of Records from the CA DOJ CII that respondent's fingerprints, whether electronic or paper, are not on file with the CA DOJ CII, or not available to the CA DOJ CII on request through other law enforcement agencies via data sharing agreements. The EC failed to describe the extent to which he was able to search and access information in the CA DOJ CII system, or what the limits were regarding what he could or could not access in support of his claim. His claim was thus hearsay, not corroborated, lacked foundation and was not supplemented or explained by other evidence.<sup>17</sup>

---

<sup>17</sup> Hearsay evidence may be used for the purpose of supplementing or explaining other evidence but is not sufficient in itself to support a finding unless it would be admissible over objection in civil actions. Government Code section 11513, subdivision (d).

25. The EC did not produce any request of the CA DOJ CII to perform a search for him on behalf of the CBA for respondent's fingerprint or CORI records, despite respondent's repeated requests in his letters to the EC and in his CPRA for any documentation of the EC's, or of any other CBA official, request of the CA DOJ CII to produce any of respondent's fingerprints, criminal history records or a CORI criminal record clearance report based on those records, on file with the CA DOJ CII.

26. The EC testified that there is no electronic record of respondent's fingerprints on file with the CBA. The EC testified that he believed that if the CBA did once have a set of respondent's rolled paper fingerprints, those fingerprints had been destroyed and were not submitted to the CA DOJ CII. He was unable to date when those actions took place. He failed to produce any official CBA action directive, order of the CBA, memoranda, notation or any other written documentation regarding who ordered the destruction of existing fingerprints on file for licensees and when that order was carried out, despite respondent's Rick repeated requests that he do so. As a result, the CBA was unable to prove that the order to destroy respondent's fingerprints on file with the CBA since 1976 was not made after respondent began to make an issue about his compliance with section 37.5 due to his previous submission of his paper fingerprints as part of his license issuance. The EC confirmed that the CBA does still permit submission of rolled paper fingerprints and does send those paper fingerprints to the CA DOJ CII for production of a CORI state and federal criminal record clearance report for the licensee submitting, for out-of-state licensees and those who do not have access to a Live Scan system.

27. The EC also testified that he spoke to Lani about her January 2015 conversation with respondent. He claimed that she denied seeing respondent's fingerprints in his personnel records when she spoke to respondent, and that she gave respondent "the standard response;" that all paper fingerprint cards obtained from licensees were not submitted to the CA DOJ and were subsequently destroyed. His testimony about what Lani told him was uncorroborated hearsay, not supplemented or explained by any other evidence. Lani did not provide a written statement or an affidavit. The EC failed to produce anything in writing by Lani that would confirm she actually said what he claimed, or that what he reported she said was complete, truthful or accurate.

28. The EC claimed to have received "a list" from the CA DOJ CII, showing all CBA licensees who have digital fingerprint records on file with the CA DOJ CII. He claimed the list was contained on three CDs, but he failed to produce this "list," or any other documentation from the CA DOJ CII that would corroborate this claim, despite repeated requests by respondent that he produce any such list or documentation supporting this claim. The EC's failure to produce any of the lists he claimed he reviewed renders it impossible to assess the nature and the quality of the data contained on the "lists," or consider that information as supporting evidence of any CBA claim or contention.

29. The EC testified that he and the EO also made "diligent" searches of information received by the CBA regarding its licensees from the CA DOJ CII, and wrote in a letter to respondent that he and the EO failed to find confirmation that respondent's digital fingerprints were on file with the CA DOJ CII. No specific document or record was ever

identified that was claimed to have been searched, other than the unidentified and unproduced "lists," referenced above. No declaration, record, report or memorandum was written by the EC or the EO describing any specifics of this "diligent" search, including what records or information were searched, where those records were kept, how they were searched, whether the information was current or stale, identification of any records that could not be searched or were unavailable, how many records were missing or incomplete, or any information beyond their vague and conclusory statements that whatever they searched they searched "diligently."

30. The EC repeatedly prefaced his testimony by stating "according to the DOJ." He repeatedly failed to produce any record or document that would provide any foundation for such a claim. His claims were vague and lacked any foundation to move the statements beyond conclusory and opinion. He failed to produce any document or record supporting that claim despite respondent's repeated requests that he do so. He was unable to identify who he spoke to at the CA DOJ, that person(s) capacity and authorization to speak for CA DOJ, and what he or she reviewed, how he or she acquired information, or what information was actually provided to the EC "according to the DOJ." This claim also appears contradictory to his testimony that he was precluded as a "third party," from obtaining information regarding respondent's fingerprints and/or criminal history from CA DOJ CII lodged by any person or entity other than the CBA, due to concern he might violate Penal Code section 11142.

31. The EC's claim he reviewed the results of "automated cross matching" between the CBA's licensee records and the CA DOJ CII's electronic fingerprint system that he claimed supported his testimony that there is no electronic fingerprint record for respondent on file with the CA DOJ CII contains similar deficits. His testimony relied entirely upon hearsay for its foundation. He failed to produce any records or documentation to corroborate or provide foundation for his claim. He was unable to answer respondent's question regarding the accuracy and completeness of the system he used for his claimed records cross matching, except to confirm that it was not 100 per cent accurate, but not as inaccurate as the over 50 percent alleged error rate of the not yet deployed BrEZE system. He was unable to describe any means by which he could reasonably assure that the data he was cross matching from the CBA and the CA DOJ CII was accurate or complete.

32. The EC failed repeatedly to adequately respond to respondent's questions seeking the basis of his claim that the CA DOJ CII does not have sufficient identifying information, and cannot produce a CORI state and federal criminal record clearance report on him that could be provided to the CBA to confirm respondent's freedom from any criminal activity. The EC claimed in his testimony and in one of his letters to respondent that the CBA is legally unable to access respondent's fingerprints, criminal history or CORI information that might be on file with the CA DOJ CII residing there due to the actions of "third parties" due to reasons other than by CBA request. The EC thus claimed the CBA cannot request a CORI state and federal criminal record clearance be produced for respondent and sent to the CBA using fingerprint or other information about respondent contained in any other law enforcement database, such as the US DHS, US DOJ or FBI, or by use of a Live Scan digital fingerprint received as part of a criminal history background



check for authorization to become a Trusted Traveler in Global Entry. The EC testified he had been advised by "legal counsel" that Penal Code section 11142 prohibits the CBA from accessing fingerprints and other criminal record information about CBA licensees that CA DOJ CII holds as a result of fingerprints and other information being submitted to the CA DOJ CII by "third parties," such as another licensing or law enforcement agency. He agreed he had no legal opinion or anything in writing expressing this legal position. He failed to identify the legal counsel who provided the opinion. He failed to explain how he understood Penal Code section 11142 would preclude the CBA from accessing upon request respondent's electronic fingerprint information contained in the US DHS data base from his Global Entry application, that may also reside in the CA DOJ CII data base, or the results of the US DHS criminal records search and clearance of respondent's identifying information against his CA DOJ CII records for Global Entry.

33. The EC claimed that it was his opinion that respondent could not provide the CBA effective written authorization to access his digital fingerprint and CORI information contained in any other law enforcement database. His opinion lacked foundation, was speculative and unpersuasive. He claimed but failed to explain how Penal Code section 11124 would bar the CBA's access to respondent's fingerprint information where respondent has authorized the CBA to have that access in writing. His opinion and testimony amounted to a legal opinion on behalf of the entities holding and responsible for providing access to the records sought, such as the CA DOJ CII, the US DHS, the US DOJ and/or the FBI, and a legal opinion expressed on behalf of the person(s) or entities in charge of access to respondent's information contained in any other law enforcement database who might receive and be called upon to act upon such an authorization.

34. Respondent testified credibly and persuasively regarding his understanding of his obligations to the CBA as a licensee, and of his recognition of and responsiveness to the CBA's need to have access to and the ability to receive a CORI state and federal criminal history clearance report, based upon use of his fingerprints to identify him to his records on file with the CA DOJ CII, as well as on those file with any other law enforcement agencies, such as the US DHS, US DOJ or FBI.

35. Respondent pointed out that he is certain of at least one federal law enforcement agency does have a full set of his digital fingerprints captured quite recently, as well as the results of a recent, comprehensive criminal record background check that required a state, federal and international law enforcement criminal record clearance. He testified that he provided his fingerprints via Live Scan to the US DHS in January 2013 at the San Francisco International Airport to officials of the US Border Protection and Customs Service, a branch of the US DHS, as part of his application and approval to participate in the Global Entry Trusted Traveler program. He claimed that those electronic fingerprints he provided, and the state, federal and international criminal record clearance from Global Entry produced as a result of the US DHS using those electronic fingerprints as identifying data, also reside in the CA DOJ CII, US DOJ and FBI criminal history databases due to the requirement that all of these databases be searched in order to complete the clearance, and that these law enforcement agencies share data for the purposes of completing criminal background checks. Respondent's claim was not contested and was verified with documentation respondent

presented that showed he was approved as a Global Entry Trusted Traveler, which necessarily confirmed that his comprehensive state, federal and international criminal record inquiry was clear.

36. Respondent reiterated in his testimony his offer to provide written authorization to the CBA to obtain a copy of his Live Scan digital fingerprint he submitted to the US DHS in conjunction with his application for Global Entry, or any fingerprints that reside in the CA DOJ CII, US DHS, US DOJ or FBI databases. Alternatively, he continued in his testimony his previously and repeatedly stated offer to the CBA to obtain and submit a set of Live Scan fingerprints within 30 days of a determination regarding the merits of his contention that he should be found in compliance with section 37.5. He firmly believes that he should not have to pay for and submit to yet another Live Scan when he has just completed one, especially where his fingerprints were filed with the CBA in 1976 and should have been still available to the CBA to run any criminal background check on him it desires, had those fingerprints not been destroyed without notice. He contends that the CBA's legal opinion about the impediment of Penal Code section 11142 to his ability to authorize access to his electronic fingerprints and criminal records is not correct, and that since he is the person whose identifying information is the subject of the request, he is legally permitted to provide that access in writing.

37. Respondent believed up until very recently that the CBA had retained his rolled paper fingerprints that he submitted as part of his application in 1976, and it came as a surprise that the CBA would destroy those fingerprints without notice to him or other licensees, rather than submit them to the CA DOJ CII. He continues to contend that he complied with section 37.5, because he submitted his fingerprints in 1976, regardless of what the CBA did with those fingerprints after he submitted them, and that he should not be found in noncompliance because of the CBA's unilateral decision to destroy his fingerprints. He contends the CBA confirmed receipt of his paper fingerprints by issuing his CPA license, presumably after using those fingerprints to conduct a criminal record background check and obtain a CORI state and federal criminal record clearance report, to confirm that he did not have any disqualifying criminal record. He also contends that those fingerprints must have remained on file with the CBA for many years, otherwise there would have been no identifying information available for the CBA to continue to check and crossmatch his records at the CA DOJ CII for each of his numerous biannual renewals. He further expressed surprise at the EC's claim in his testimony that in all the years from 1976 through his most recent biannual renewal, that, if his fingerprints had not been submitted to the CA DOJ CII, his criminal history could not have been checked, nor could a CORI criminal record clearance report to the CBA have been generated, confirming that he had no criminal history at each of his biannual renewals. He also expressed disappointment that the CBA did not notify licensees such as him who had paper fingerprints on file with the CBA that the CBA intended to destroy the fingerprints, and failure to provide him and his fellow licensees with options on how to use those paper fingerprints, including giving licensees the option of paying for the cost themselves of submitting those paper fingerprints to the CA DOJ CII for digitization.

## LEGAL CONCLUSIONS

1. Business and Professions Code section 125.9 provides that the CBA may establish, by regulation, a system for the issuance to a licensee of a Citation which may contain an Order of Abatement or an Order to pay an Administrative Fine. In assessing a fine, the Board shall give due consideration to the appropriateness of the amount of the fine with respect to factors such as the gravity of the violation, the good faith of the licensee, and the history of previous violations.

2. California Code of Regulations, title 16, section 95, provides that the CBA's Executive Officer may issue a Citation to any person who holds a permit or certificate from the CBA for a violation of any provision of the Accountancy Act or any regulation adopted by the CBA. California Code of Regulations, title 16, section 95.2 provides that the amount of the administrative fine assessed by the Executive Officer shall not be less than \$100 or more than \$5,000 for each investigation.

3. Business and Professions Code section 144 provides, in part:

(a) Notwithstanding any other provision of law, an agency designated in subdivision (b) shall require an applicant to furnish to the agency a full set of fingerprints for purposes of conducting criminal history record checks. *Any agency designated in subdivision (b) may obtain and receive, at its discretion, criminal history information from the Department of Justice and the United States Federal Bureau of Investigation.*

(b) Subdivision (a) applies to the following:

(1) *California Board of Accountancy.*  
(Emphasis added.)

4. Business and Professions Code section 144.5 provides, in part

*Notwithstanding any other law,*<sup>18</sup> a board described in Section 144 may request, and is authorized to receive, *from a local or state agency* certified records of all arrests and convictions, certified records regarding probation, *and any and all other related documentation needed to complete an applicant or licensee investigation. A local or state agency may provide those records to the board upon request.* (Emphasis added.)

5. The CBA is, and has been at all times relevant to this Decision, and since at least 1997, the date of enactment of sections 144 and 144.5 above, required to obtain a full

---

<sup>18</sup> Including, presumably, Penal Code section 11142.

set of fingerprints from every applicant for a CPA license before issuing the license, as required by statute, sections 144 and 144.5 above. Compliance via submission of paper rolled fingerprints before the advent of electronic fingerprints capture, and to date for those who do not have access to Live Scan or live out of state, has been permitted, as the CBA acknowledged in its Statement of Reasons and in the October, 2000 newsletter article to licensees about fingerprinting, where licensees were advised that they were provided two paper fingerprint cards by the CBA with their applications for the obtaining and submission of such fingerprints in non-electronic form. The CBA has been requiring fingerprint submission and a criminal record clearance as a condition of issuance of a CPA license long before the enactment of sections 144 and 144.5 or the advent of electronic fingerprint capture. Respondent's 1976 CBA application for licensure as a CPA in evidence confirms this, as does the article advising licensees about fingerprinting in the CBA's October 2000 newsletter. The CBA undertook fingerprinting and obtaining criminal record clearances as a condition of initial licensure as a CPA as an official duty. That official duty included obtaining respondent's fingerprints and obtaining a criminal record clearance on him at the time it issued him his license in 1976. An official duty is presumed to have been regularly performed,<sup>19</sup> therefore it must be presumed that the CBA did, as opposed to "may have," required respondent, as he claimed, to submit a full set of fingerprints in 1976 as part of his initial licensure. Respondent credibly testified that he submitted a full set of rolled paper fingerprints to the CBA as part of his initial licensure. It is also reasonable to assume that those fingerprints remained on file with the CBA for an indefinite period thereafter, and were used to cross reference with respondent's records at the CA DOJ CII in order to biannually confirm that respondent's criminal record remained crime free in order to approve his license renewals. There was no credible evidence to the contrary. There was no evidence when respondent's fingerprints and records of their submission were destroyed.

## CONSTRUCTION AND APPLICATION OF SECTION 37.5

6. The CBA contends in the Citation that respondent violated section 37.5 because in his most recent license renewal application, he failed to "successfully complete a state and federal level criminal offender record information search conducted through the Department of Justice by the licensee's renewal date that occurs after December 31, 2013," which, in effect, actually charges respondent failed to submit a new set of fingerprints in electronic form via Live Scan, and that section 37.5 requires him to do so because the CBA does not have his electronic fingerprints on file. The CBA told respondent how it was interpreting the requirements of section 37.5 as they applied to him through its EC's March 30, 2015 letter, advising respondent that he was in violation of section 37.5 because:

... Even if the licensee completed the fingerprint process as a condition for licensure, if no electronic record of the licensee's fingerprints exists with the DOJ, the licensee must still submit the fingerprints as a condition for license renewal.

---

<sup>19</sup> Evidence Code section 664. This presumption was also applied to the acts of the CBA's EC and EO. The presumption is rebuttable. The presumption is rebutted where there exists evidence that official duties performed were not factually or legally correct.

7. The CBA's Statement of Reasons supporting adoption of section 37.5 offers a different interpretation in the comment section, reading the two clauses of section 37.5, subdivision (a) disjunctively. The CBA's Statement of Reasons provides, in its response to comments by Mr. Gai as set forth in the Factual Findings:

Due to the fact that the language is clear that a licensee applying for renewal must submit fingerprints *in two cases*;

1. When the licensee has not previously submitted fingerprints as a condition of licensure, *or*
2. When an electronic record of the licensee's fingerprints does not exist in the Department of Justice's criminal offender record identification database. (Emphasis added.)

8. Respondent contends and the language of subdivision (a) supports the Statement of Reasons' comment that the provision creates an either or compliance mechanism; either the licensee has previously submitted his fingerprints or must do so with licensure or renewal. Respondent's previous submission of his paper fingerprints to the CBA in 1976, prior to the age of digital fingerprint capture and storage, satisfies the first of the two disjunctive alternatives for compliance set forth in section 37.5, subdivision (a). Respondent contends that if the CBA intended section 37.5, subdivision (a) to mean what it was claimed to mean in the EC's March 30, 2015 letter and in the CBA's argument in support of the allegations of the Citation, the provision should have expressly said so. Respondent's contention has merit. The CBA's contention lacks proof.

9. California Code of Regulations, title 16, section 37.5 is most easily interpreted by breaking it apart at the conjunctions that connect its component clauses, in similar fashion to the manner in which the CBA responded to Mr. Gai's comments in the Statement of Reasons. Subdivision (a) provides:

(a) A licensee applying for renewal as a certified public accountant or public accountant who has *not* previously submitted fingerprints as a condition of licensure

*or*

for whom an electronic record of the licensee's fingerprints does not exist in the Department of Justice's criminal offender record identification database shall successfully complete a state and federal level criminal offender record information search conducted through the Department of Justice by the licensee's renewal date that occurs after December 31, 2013.

(1) A licensee shall retain for at least three years as evidence of having complied with subdivision (a) either a receipt showing

that he or she has electronically transmitted his or her fingerprint images to the Department of Justice *or, for those who did not use an electronic fingerprint system, a receipt evidencing that his or her fingerprints were recorded and submitted to the board.* (Emphasis added.)

10. The key portions of section 37.5, subdivision (a) are the words “or,” and “not.” The plain meaning of the use of the disjunctive “or” in the provision means that respondent can comply with the requirements of subdivision (a) by proving that *either* he meets the first or the second of the alternative requirements of subdivision (a). The first clause of subdivision (a), before the word “or,” requires submission of electronic fingerprints by any “licensee applying for renewal as a certified public accountant or public accountant who *has not previously submitted fingerprints* as a condition of licensure.” The “not” is cumbersome but critical, because it includes in the class of licensees required to submit new electronic fingerprints those who have “not” previously submitted fingerprints to the CBA. Respondent has previously submitted fingerprints to the CBA, so he is not a person who “has not previously” submitted fingerprints as a condition of licensure. Respondent is therefore not a person included in the class of people who are required by the second clause of section 37.5, subdivision (a), after the “or,” to submit new electronic fingerprints as a condition of renewal.

11. The CBA’s interpretation of subdivision (a) requires respondent to meet the requirements on both sides of the “or,” because the CBA destroyed his fingerprints. The CBA’s contention in effect means its destruction of respondent’s previously provided fingerprints should operate as a de facto reversal of respondent’s compliance with section 37.5, subdivision (a). There was no evidence of any intention to authorize the CBA through section 37.5 to disqualify a licensee who otherwise met the requirements of subdivision (a) by unilateral destruction of the licensee’s means for that qualification. Respondent’s compliance with the requirements of the first clause of section 37.5, subdivision (a), because he previously submitted his fingerprints as a condition of licensure, cannot be reversed if the CBA later decides to destroy respondent’s fingerprints. Subdivision (a) contains no language, express or implied, that may be fairly interpreted to require respondent to submit new electronic fingerprints after he already submitted his fingerprints as a condition of licensure, satisfying the requirements of the first clause of subdivision (a), where the CBA later caused those fingerprints to be removed from respondent’s licensing records without notice to him. Respondent does not become subject to the requirements of the second clause of subdivision (a) and become a person who has not previously submitted his fingerprints, when he did previously submit them, just because the CBA later destroyed them.

#### PAPER FINGERPRINTS AND DESTRUCTION OF RECORDS

12. Respondent’s claim that section 37.5, subdivision (a) assumes that the CBA will retain fingerprints, even those in paper rolled form on fingerprint cards, submitted by licensees as part of their initial licensure or renewal is reasonable, and was not rebutted by any evidence presented by the CBA. The reasonableness of respondent’s assumption is bolstered by section 37.5’s specific provision “for those who did not use an electronic

fingerprint system,” requiring the licensee that submits his or her fingerprints recorded by a non-electronic fingerprint system to demonstrate that those non-electronic fingerprints were submitted to the CBA.

13. The law disfavors interpretations of provisions that lead to absurd or contradictory results.<sup>20</sup> The first clause of subdivision (a) of section 37.5 is superfluous, if persons like respondent, who submitted their fingerprints to the CBA in paper rolled form, cannot comply without submitting another set of electronic fingerprints. The first clause of subdivision (a) of section 37.5 is meaningless if the licensee who submits fingerprints in non-electronic form cannot reasonably assume that the CBA will retain those fingerprints in their records, not destroy them, and later demand those prints be resubmitted in electronic form. Section 37.5, subdivision (a) makes no mention of a requirement that mandates all licensees who have “previously submitted his fingerprints to the CBA as a condition of licensure” in paper rolled form still must resubmit their fingerprints in electronic form in order to renew, despite the fact that they have previously submitted their fingerprints in non-electronic form if the CBA fails to retain those previously submitted fingerprints. In fact, such an interpretation would conflict with the portion of the provision quoted just above that specifically provides for compliance by licensees who have provided fingerprints in non-electronic form to the CBA and assumes those fingerprints will be retained.

14. The first clause of section 37.5, subdivision (a) does not say that the licensee applying for renewal who has previously submitted fingerprints as part of the licensure process must have submitted those fingerprints in electronic form or through Live Scan. The language of the regulation is not so restrictive, and permits compliance through previous submission of fingerprints in both paper and electronic form, making no distinction.

15. The CBA failed to prove that respondent violated section 37.5, as set forth in the Factual Findings. The CBA failed to prove two key elements of the violation required by subdivision (a). The CBA failed to prove that respondent is not a person who meets the requirements of the first clause of subdivision (a), a person who has not previously submitted his fingerprints to the CBA as part of his initial licensure, as set forth in the Factual Findings. The CBA failed to prove that it is unilateral, unnoticed destruction of respondent’s fingerprints previously submitted to the CBA renders his previous compliance a nullity.

#### ACCESS TO RESPONDENT’S FINGERPRINT RECORDS

16. Penal Code section 11140 provides, in part:

As used in this article:

(a) ‘Record’ means the state summary criminal history information as defined in subdivision (a) of Section 11105, or a copy thereof, maintained under a person’s name by the Department of Justice.

---

<sup>20</sup> *Lungren v. Deukmejian* (1988) 45 Cal.3d 727, 735.

(b) ‘A person authorized by law to receive a record’ means *any person or public agency authorized by a court, statute, or decisional law to receive a record*. (Emphasis added.)

17. Penal Code section 11124 provides, in part:

When an application is received by the department, the department shall determine whether a record pertaining to the applicant is maintained. If such record is maintained, the department shall furnish a copy of the record *to the applicant or to an individual designated by the applicant*. If no such record is maintained, the department shall so notify the applicant or an individual designated by the applicant. Delivery of the copy of the record, or notice of no record, may be by mail or other appropriate means agreed to by the applicant and the department. (Emphasis added.)

18. Penal Code section 11105, subdivision (b)(10) provides:

The Attorney General shall furnish state summary criminal history information to any of the following, if needed in the course of their duties ....

(10) *Any agency, officer, or official of the state if the criminal history information is required to implement a statute or regulation that expressly refers to specific criminal conduct applicable to the subject person of the state summary criminal history information, and contains requirements or exclusions, or both, expressly based upon that specified criminal conduct. The agency, officer, or official of the state authorized by this paragraph to receive state summary criminal history information may also transmit fingerprint images and related information to the Department of Justice to be transmitted to the Federal Bureau of Investigation*. (Emphasis added.)

19. The CBA failed to prove that respondent is not a person “for whom an electronic record of the licensee’s fingerprints does not exist in the Department of Justice’s criminal offender record identification database,” as required by the second clause of section 37.5, subdivision (a). The CBA failed to prove that the CA DOJ CII cannot access an electronic record of respondent’s fingerprints and produce a CORI state and federal criminal history report to the CBA, either through its authority to conduct a legitimate law enforcement criminal record background check, authorized by Penal Code section 11105, subdivision (b)(10) and Business and Professions Code sections 144 and should 144.5, or, alternatively, upon respondent’s repeatedly offered written authorization to permit access to respondent’s fingerprint information that exists at least in the federal law enforcement database of the US DHS.



20. Section 11124 above clearly contemplates the ability of the person whose fingerprints exist in a law enforcement database to authorize access to and disclosure of those fingerprints to or by the CA DOJ CII and to or by the CBA. The CBA's evidence in support of its claim was unpersuasive hearsay and hearsay on hearsay, uncorroborated by any records or documents. The CBA did not offer a Penal Code section 11124 Declaration of Nonexistence of Records from the CA DOJ CII stating either; 1. That that no fingerprint records exist for respondent in the CA DOJ CII database that may be accessed by the CBA upon respondent's authorization, or are reasonably available through data sharing arrangements with federal law enforcement agencies in their databases, or 2. That respondent is a person "for whom an electronic record of the licensee's fingerprints does not exist in the Department of Justice's criminal offender record identification database."

#### THE PENAL CODE SECTION 11142 PRECLUSION CLAIM

21. Penal Code section 11142 provides:

Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person ***who is not authorized by law to receive the record or information*** is guilty of a misdemeanor.  
(Emphasis added.)

22. The CBA's EC's claim in his testimony that information sharing between the CBA, the CA DOJ CII and US DHS is unlawful, and access to that information cannot be authorized by respondent in favor of the CBA, because such sharing constitutes unauthorized access to "third party" data, constituting a misdemeanor, lacks legal support, and misconstrues section 11142. The only person or entity subject to the threat of a criminal violation of section 11142 is a person or entity that furnishes access to or provides records or information without legal authorization, or to a person who is not authorized by law to receive it.

23. The CA DOJ CII is statutorily authorized by Penal Code section 11105, subdivision (b)(10) and Business and Professions Code section 144.5, ("notwithstanding any other provision of law") to provide, upon the CBA's request, respondent's state and federal criminal history that exists for respondent for the purpose of conducting a statutorily required licensee background check. The key to accessing that information is respondent's fingerprints as his identifier. Respondent previously submitted his fingerprints to the CBA, and was entitled to reasonably believe that the CBA would retain that information for use to correlate against his CA DOJ CII records for the purpose of producing a CORI. There was no evidence, nor did the CBA claim, that paper rolled fingerprints such as respondent submitted could not be used for the purpose of identifying him and checking his records by the CA DOJ CII, or in producing a CORI. In the absence of the CBA retaining respondent's fingerprints, respondent has offered to provide written access to his electronic fingerprints, captured in January 2013, on file with the US DHS, as well as to the results of his US DHS Global Entry comprehensive criminal record background check, fingerprints and records that are likely on file with the CA DOJ CII as well.

24. Penal Code section 11142 does not prohibit criminal record data sharing between agencies conducting licensee criminal record background checks. It says nothing about a person whose data it is, in this instance, respondent, being precluded from authorizing access to data pertaining to him contained in state or federal law enforcement databases to an agency like the CBA conducting a Penal Code section 11105, subdivision (b)(10) lawful criminal background check. Penal Code section 11142 does not preclude an agency named in Business and Professions Code section 144, such as the CBA, from requesting and accessing criminal history records from the CA DOJ CII for a legitimate law enforcement purpose, such as that set forth in Penal Code section 11105, subdivision (b)(10), such as for purposes of licensing investigation and conducting criminal history background checks. The provisions just above make clear that both the CBA and the CA DOJ CII are authorized to send and receive respondent's fingerprint information as part of the CBA's statutory duty to conduct criminal record background checks of licensees, and that respondent is a person who can authorize access to any such record that was put into a law-enforcement database at a request of a party other than the CBA in favor of an agency like the CBA performing a legitimate law enforcement task with that access.

25. Respondent acknowledges the CBA's need to accomplish its public protection purpose, but pointed out that the CBA's public protection purpose is more than satisfied through the results of his submission to a US DHS Global Entry Trusted Traveler comprehensive criminal record background check and clearance. Respondent's claim has merit. Respondent's US DHS Global Entry Trusted Traveler criminal record background check in January 2013 included his submission of a Live Scan set of electronic fingerprints that were used to crosscheck his identity with state, federal and international databases maintained by the CA DOJ CII (for the state level criminal record clearance check), US DHS, US DOJ, FBI (for the federal level criminal record clearance check) and Interpol (for the international level criminal record check). Respondent complied with the first clause of section 37.5, subdivision (a), as set forth above, but despite that, he has repeatedly offered the CBA written authorization to access all of the data obtained and maintained on him through the comprehensive criminal record background check he submitted to and passed, conducted by the US DHS, as evidenced by receiving his approval to participate in Global Entry as a Trusted Traveler on January 31, 2013. Respondent's offer constitutes a reasonable alternative to meet the objectives of section 37.5, since the CBA failed to prove the allegations in the Citation. It is unreasonable to conclude that accepting respondent's offer to obtain and use written access to his electronic fingerprints and comprehensive criminal record background check maintained in these federal databases is not an adequate alternative to meet the CBA's public protection mandate for respondent's license renewal, expressed in Business and Professions Code sections 144 and 144.5 above.

#### EQUITABLE ESTOPPEL

26. Respondent contends he has been disadvantaged because the CBA claims to have destroyed his fingerprints he submitted, and that the CBA claimed those fingerprints were not submitted to the CA DOJ CII for deposit into their CII database and later digitization, all without notice to himself and others similarly situated licensees who submitted their fingerprints in paper copy. The CBA's failure to preserve respondent's

fingerprints submitted as part of his initial licensure, and the CBA's destruction of those fingerprints without notice to respondent, and without providing an opportunity for those fingerprints to be submitted to the CA DOJ CII, where they could have been digitized and retained in the CA DOJ CII database, has prejudiced respondent and, as set forth above, had the effect of causing the CBA to complain that he is not compliant with section 37.5, subdivision (a) because his paper fingerprints no longer reside in his CBA licensing file. Had the CBA, or alternatively, respondent, after having received notice from the CBA of the potential destruction of his fingerprints on file with the CBA, submitted those fingerprints to the CA DOJ CII for digitization and retention, respondent's fingerprints would have been available to use for cross matching and production of a CORI state and federal criminal record clearance report to the CBA, making compliance with section 37.5 here a non-issue. Had those fingerprints been scanned and digitized, cross matching the scanned fingerprints and using them as a tool for verifying respondent's identity with his records on file with the CA DOJ CII would have been routine.

27. Generally speaking, four elements must be present in order to apply the doctrine of equitable estoppel: (1) the party to be estopped must be apprised of the facts; (2) he must intend that his conduct shall be acted upon, or must so act that the party asserting the estoppel had a right to believe it was so intended; (3) the other party must be ignorant of the true state of facts; and (4) he must rely upon the conduct to his injury."<sup>21</sup> "Correlative to this general rule, however, is the well-established proposition that an estoppel will not be applied against the government if to do so would effectively nullify 'a strong rule of policy, adopted for the benefit of the public, . . .'"<sup>22</sup> Whether the injustice which would result from a failure to uphold an estoppel is of sufficient dimension to justify the effect of the estoppel on the public interest must be decided by considering the matter from the point of view of a court of equity."<sup>23</sup>

28. The CBA's claim, without any supporting records, that it does not have fingerprints on file for respondent, or access to his fingerprints he submitted in 1976, is the product of its own action, destroying respondent's fingerprints without notice. The CBA's action deprived respondent of the ability to be in compliance with section 37.5 without further unnecessary costs or the effort to obtain another, superfluous Live Scan. Respondent should not be penalized for the consequences of the CBA's own internal decision to destroy respondent's fingerprints. The paramount public policy served by requiring submission of fingerprints in order to conduct criminal record background checks is not defeated by

---

<sup>21</sup> *City of Long Beach v. Mansell* (1970) 3 Cal.3d 462, 487, *Driscoll v. City of Los Angeles* (1967) 67 Cal.2d 297, 305.

<sup>22</sup> *Id.*

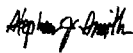
<sup>23</sup> *Id.*, at pp. 496-97, *Smith v. County of Santa Barbara* (1992) 7 Cal.App.4<sup>th</sup> 770, 775.

estopping the CBA from penalizing respondent in this case, because there are reasonable alternatives to obtain the information and accomplish the public policy purpose without penalizing respondent. The tests of *Mansell*, *Driscoll* and *Smith* are met. The CBA is estopped from penalizing respondent through the Citation for failing to submit to a new Live Scan, as required by the Order of Abatement, and for penalizing him for failing to do so.

ORDER

Citation No CT-2016-1 is DISMISSED.

DATED: February 5, 2016

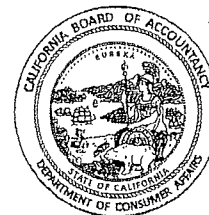
DocuSigned by:  
  
25D4275E07F6483...

---

STEPHEN J. SMITH  
Administrative Law Judge  
Office of Administrative Hearings



DEPARTMENT OF CONSUMER AFFAIRS  
CALIFORNIA BOARD OF ACCOUNTANCY  
2000 EVERGREEN STREET, SUITE 250  
SACRAMENTO, CA 95815-3832  
TELEPHONE: (916) 263-3680  
FACSIMILE: (916) 263-3675  
WEB ADDRESS: <http://www.cba.ca.gov>



## CITATION ORDER

Ned Alan Leiba  
305 N. El Dorado #302  
Stockton, CA 95202

Citation No. CT-2016- 1  
License No. CPA 23912

The California Board of Accountancy (CBA) conducted an investigation and is issuing this citation pursuant to Business and Professions Code, Sections 125.9 and 5100, and Title 16, California Code of Regulations, Sections 95 – 95.6.

This citation details each violation charged and orders of correction where applicable. **It is the licensee's responsibility to read the entire citation.**

Unless contested, this citation shall become a final order of the CBA on July 31, 2015; the Order of Correction is due on or before July 31, 2015; and the administrative fine totaling \$500 is due on or before July 31, 2015.

The licensee is responsible for notifying the CBA when correction is made. Proof of correction must be received at the above address no later than five (5) working days after the correction due date.

Payment of the administrative fine should be made to the CBA by Cashier's Check or Money Order. Please include the citation number on the payment and on all correspondence.

**Failure to respond to this citation may result in disciplinary action against the license.**

6/26/2015  
Date

Patti Bowers  
Patti Bowers  
Executive Officer  
CALIFORNIA BOARD OF ACCOUNTANCY

PB:JL

Attachments: Statement to Cited Licensee  
Notice of Appeal  
Government Code Sections 11507.5, 11507.6, and 11507.7

**Item No. 1**

**Section(s)  
Violated:**

CALIFORNIA CODE OF REGULATIONS  
TITLE 16. Professional and Vocational Regulations  
DIVISION 1. Board of Accountancy Regulations  
ARTICLE 5. Registration

**SECTION 37.5. Fingerprint and Disclosure Requirements.**

(a) A licensee applying for renewal as a certified public accountant or public accountant who has not previously submitted fingerprints as a condition of licensure or for whom an electronic record of the licensee's fingerprints does not exist in the Department of Justice's criminal offender record identification database shall successfully complete a state and federal level criminal offender record information search conducted through the Department of Justice by the licensee's renewal date that occurs after December 31, 2013.

(1) A licensee shall retain for at least three years as evidence of having complied with subdivision (a) either a receipt showing that he or she has electronically transmitted his or her fingerprint images to the Department of Justice or, for those who did not use an electronic fingerprint system, a receipt evidencing that his or her fingerprints were recorded and submitted to the board.

(2) An applicant for renewal shall pay the actual cost of compliance with subdivision (a).

(3) As a condition of petitioning the board for reinstatement of a revoked or surrendered license, an applicant shall have complied with subdivision (a).

(4) The board shall waive the requirements of this section if the license is renewed in an inactive or retired status or if the licensee is actively serving in the United States military. The board shall not return a license to active status until the licensee has complied with subdivision (a).

(b) As a condition of renewal, a certified public accountant or public accountant licensee shall disclose on the renewal form whether he or she has submitted a record of fingerprints in compliance with subdivision (a).

(c) As a condition of renewal, an applicant for renewal as a certified public accountant or public accountant shall disclose on the renewal form whether he or she has been convicted, as defined in Section 490 of the Business and Professions Code, of any violation of the law in this or any other state, the United States, or other country, omitting traffic infractions under \$1000 not involving alcohol, dangerous drugs, or controlled substances.

(d) As a condition of renewal, an applicant for renewal as a certified public accountant or public accountant shall disclose on the renewal form whether he or she has experienced the cancellation, revocation, or suspension of a certificate or right to practice by any other state or foreign body.

(e) Failure to provide all of the information required by this section renders an application for renewal incomplete and the license will not be renewed until the licensee demonstrates compliance with all requirements.

**Description  
of Violation:**

Ned Alan Leiba failed to complete a state and federal level criminal offender record information search by submitting fingerprints prior to renewing his license in an active status for the renewal period that ended September 30, 2014.

**Order of  
Abatement:**

Comply with all CBA statutes and regulations.

**Order of  
Correction:**

- Complete a criminal offender record information search conducted by the Department of Justice.
- Pay the administrative fine as set forth in the citation.

**Time to  
Correct:**

30 days / By July 31, 2015

**Administrative  
Fine:**

\$500