COM/LR1/lil

PROPOSED DECISION

Agenda ID #16025 (Rev. 2)
Quasi-legislative
11/9/2017, Item #17

Decision **PROPOSED DECISION OF COMMISSIONER RANDOLPH**
(Mailed 10/4/2017)

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA

Order Instituting Rulemaking on Regulations Relating to Passenger Carriers, Ridesharing, and New Online-Enabled Transportation Services.	Rulemaking 12-12-011

PROPOSED DECISION ON PHASE III. B. ISSUE: CRIMINAL BACKGROUND CHECKS FOR TRANSPORTATION NETWORK COMPANY DRIVERS

Table of Contents

Title **Page**

PROPOSED DECISION ON PHASE III. B. ISSUE: CRIMINAL BACKGROUND CHECKS FOR TRANSPORTATION NETWORK COMPANY DRIVERS

Summary

In Decision 13-09-045, the Commission formulated background-check requirements that harmonized the goal of public safety with the public demand for the then-nascent Transportation Network Company (TNCs or TNC) services. The Commission has revisited the issue in subsequent phases of this proceeding as more information regarding the TNC industry has become available.

The California Legislature has also weighed in and established background checks that TNCs must undertake. With the enactment of Assembly Bill (AB) 1289, codified in Pub. Util. Code § 5445.2, TNCs are required to adhere to a three-part background protocol. Yet in passing AB 1289, the Legislature made it clear that its requirements were not exhaustive standards, and that the Commission maintained the authority to adopt additional standards that did not conflict with the Legislature's directive.

As such, any TNC that wishes to conduct transportation service in California must meet the requirements of Pub. Util. Code § 5445.2, which we set forth as follows:

- A TNC or a third party working on the TNC's behalf must perform a search of a multistate and multi-jurisdiction criminal records locator or other similar commercial nationwide database with validation; and conduct a search of the United States Department of Justice National Sex Offender Public Web site.
- A TNC may not contract with, employ, or retain persons currently registered on the Department of Justice National Sex Offender Public Web site; or convicted of either a violent felony or a violation of Penal Code §§ 11413, 11418, 11418.5, or 11419.
- A TNC may not contract with, employ, or retain persons convicted of any of the following offenses within the previous seven years: misdemeanor assault or battery; domestic violence offense; driving under the influence of alcohol or drugs; a felony violation of Elections Code § 18540, or Penal Code §§ 67, 68, 85, 86, 92, 93, 137, 138, 165, 518, 530, 18500, 484(a), 487(a), or 25540(b).

- Pursuant to Pub. Util. Code § 5445.2(a)(5), nothing in Pub. Util. Code § 5445.2 shall be interpreted to prevent a TNC from imposing additional standards.

In addition to the requirements set forth in Pub. Util. Code § 5445.2, the Commission exercises its regulatory authority to require every licensed TNC to comply with the following additional requirements:

> First, commercial background check companies that a TNC employs must be accredited by the National Association of Professional Background Screener's Background Screening Credentialing Council. If a TNC conducts background checks in-house, the TNC must itself be accredited by the same entity.
>
> Second, each TNC must receive proof of accreditation of the background check company and provide proof of accreditation with any reporting that the Commission may require.
>
> Third, the background screening for each TNC driver must be conducted prior to the granting of authorization to operate on the TNC's platform and repeated at least once per year thereafter, for as long as the TNC driver is authorized to operate on the TNC's platform. The TNC must provide proof of annual screening of its drivers with any reporting that the Commission may require.
>
> Fourth, we limit the information a TNC can require from a criminal background check going past seven years to those disqualifying categories of offenses and convictions set forth in Pub. Util. Code § 5445.2. We do not limit the information a TNC can obtain regarding a TNC driver applicant within the previous seven years.
>
> Finally, the Commission declines to require a TNC that does not primarily transport minors to conduct a biometric (i.e., the use of a person's physical characteristics and other traits) background check of a TNC driver.
>
> This proceeding remains open.

1. Background

1.1. The Order Instituting Rulemaking

Since initiating this proceeding to establish regulations over the then-nascent Transportation Network Company (TNCs or TNC) industry, the Commission has sought to formulate the appropriate level of background-check regulations that each TNC should

perform on its drivers. In confronting this issue, the Commission has sought to balance the need to adopt regulations that promote the public safety aspects of the TNC industry, yet not obstruct the public's demand for this new mode of transportation.

Pursuant to Ordering Paragraph 19 of Decision (D.) 16-04-041, the Scoping Memo and Ruling dated October 26, 2016, and later amended on June 12, 2017, opened a Phase III in this proceeding. The purpose behind Phase III was to explore those issues that were unresolved in Phases I and II, and to consider how best to address the advent of new issues attendant to the provision of TNC services in order to maintain the safety of TNC passengers and TNC drivers, as well as other drivers or pedestrians who may come in contact with TNC drivers. This rulemaking has sought and received comments from the parties, and has welcomed comments from the public that were either made at Commission public meetings or provided in writing to the Commission's Public Advisor's Office.

Because the Commission wanted to expand the opportunities for the public to express their opinions on the background check issue and as part of its commitment to increasing the public's involvement in its proceedings, the Commission implemented an online platform whereby the public could participate in a survey and voice their opinions on whether the Commission should require TNCs to conduct a biometric background check of current and prospective TNC drivers. Since June of 2016, the Commission has received a total of 1,817 comments on whether TNC drivers should be subject to fingerprinting as part of the background check, and the breakdown of the responses is as follows:

Yes	**No**	**It depends**	**Undecided**
879	897	34	7
48.38%	49.37%	1.87%	.039%

The survey respondents appear to be evenly divided on fingerprinting TNC drivers, and so no matter how the Commission resolves the question, many persons who responded to the survey may not be satisfied with the Commission's ultimate decision. Despite this apparent split of opinion, the Commission must base its decision on background checks with the goal of promoting public safety.

1.2. The June 26, 2016 Assigned Commissioner's Ruling

As the Commission continues to develop regulations for the TNC industry, one unresolved question is what background checks the Commission should require permitted TNCs that do not primarily transport minors[1] to perform on both their existing and prospective drivers. Previously, on June 22, 2016, the assigned Commissioner issued her *Ruling Inviting/Instructing Party Comments on Background Checks of Prospective Transportation Network Company Drivers*. On August 29, 2016, the following parties filed opening comments: HopSkipDrive, Tech Net, San Francisco International Airport (SFO) and San Francisco Metropolitan Transportation Agency (SFIA/SFMTA), California Chamber of Commerce, the Greenlining Institute, CAL Innovates, Internet Association, Rasier-CA, LLC (Rasier-CA or Rasier),[2] Engine, Lyft, Inc. (Lyft) and the San Francisco Taxi Workers Alliance (SFTWA).

1.3. Phase III.B. Scoping Memo and Ruling

The background-check inquiry was further refined in the April 7, 2017 *Phase III.B. Scoping Memo and Ruling* (*Scoping Memo and Ruling*) in which the parties were invited to address additional background-check questions in light of the California Legislature's passage of AB 1289, discussed *infra,* which established both minimum

[1] In D.16-04-041, Ordering Paragraph 6, this Commission ordered that all carriers, including TNCs, that primarily transport unaccompanied minors must comply, at a minimum, with the background check requirements articulated by this Commission in D.97-07-063.

[2] This decision refers to Rasier which is recognized by the public as Uber.

background-check protocols for TNCs, and set forth certain factors that would disqualify a person from being a TNC driver. On May 1, 2017, the following parties filed opening comments: Rasier-CA, Lyft, SFIA/SFMTA, SFTWA, and the Los Angeles Department of Transportation (LADOT).

With the advent of the TNC business, California and other states have grappled with the question of whether biometrics should be utilized as part of the background-checking process for TNC drivers.[3] As we will demonstrate, the positions of the parties fall into one of two camps—those favoring the inclusion of a biometric component as part of the background check; and those, usually the TNCs, who favor alternative background checks that do not include the biometric component and instead require a search through local, multi-state, and/or multi-national criminal records databases.[4]

While the approaches may appear different on the surface, they both attempt to accomplish the goal of conducting a comprehensive criminal history check. This conclusion was also recently reached by the Public Service Commission (PSC) of Maryland. In its December 22, 2016 *Order In the Matter of the Petitions of Rasier, LLC*

[3] As of 2016, two states have either passed legislation, or are considering legislation, requiring that fingerprinting be included as part of the background checks of TNC drivers: Maryland (PUA § 10-104(b); the law also gives a TNC the right to file a petition to waive the fingerprint-based background check [PUA § 10-404(e)(2)(ii)]); and Massachusetts introduced a bill in 2015 that would require fingerprinting. 18 states have either passed, or are considering, background check requirements that do not require fingerprinting: Arizona (Chapter 235, House Bill 21350, Colorado (Session Laws of Colorado), District of Columbia (DC Council Bill B20-0753), Georgia (House Bill 225), Illinois (SB 2774), Indiana (House Enrolled Act 1278), Nebraska (LB 629), Nevada (AB 175), New Mexico (HB 168), North Carolina (Session Law 2015-237), North Dakota (HB 1144), Ohio (HB 237), Oklahoma (HB 1614), South Carolina (H.3525), Tennessee (HB 992), Virginia (H. 1662), West Virginia (considering HB 4228), and Wisconsin (AB 143). Pursuant to Rule 13.9 and Evidence Code § 452, the Commission takes official notice of these legislative acts. A discussion of these various laws can be found in *States Address Background Checks for Rideshare Drivers*. Sean Slone February 24, 2016. The Council of State Governments.

[4] As noted above, the split of positions between the parties on whether to require fingerprinting is similar to the split of public survey opinions provided to the Commission through its online comment form.

and Lyft, Inc. For Waiver of Public Utilities Article Section 10-104(B) (*Maryland Order*), the Maryland PSC found that while no one background check process was perfect, the Rasier and Lyft background check processes were "as comprehensive and accurate as the fingerprint-based background check process under PUA § 10-104(b)."[5]

Before discussing the questions, the Scoping Memo and Ruling asked the parties to address, it will be helpful to set forth information regarding biometric background checks that California's Department of Justice (DOJ) performs, and the non-biometric background checks that TNCs such as Rasier-CA and Lyft perform. That way, the Commission can determine (1) if the current TNC background checks comply with Pub. Util. Code § 5445.2; and (2) if the DOJ's biometric background-check process adds an increased component of safety that the Commission should consider adopting.

1.4. The TNC Background-Checking Process

In Ordering Paragraph 4 of D.13-09-045, the Commission ordered each TNC to conduct a criminal background check, using the name and social security number (SSN) for each driver prior to that applicant becoming a TNC driver. We ordered that the background check be conducted on a national basis and include the national sex offender database. We also articulated certain felony criminal convictions within seven years prior to the date of the background check that would make an applicant ineligible to be a TNC driver.

In setting forth this background check requirement, the Commission declined to dictate how the process would be carried out (*i.e.* would the TNC conduct the check itself or contract with a third-party service), nor did we set forth eligibility criteria for the use of third-party background checking services. Instead, as part of the TNC application process, we required each TNC to describe its background check requirements, and

[5] *Maryland Order* at 19. Pursuant to Rule 13.9 and Evidence Code § 452, the Commission takes official notice of the *Maryland Order*.

required each TNC applicant using a background check company to submit a signed contract with that background check company.[6] The Commission's Transportation Enforcement Branch (TEB) reviews each TNC's background check process to ensure each TNC is in compliance with the Commission's orders before receiving a permit to operate in California. The continued growth in the TNC industry, as well as the recent legislative mandate, have made it necessary that the Commission take a fresh look at each TNC's processes in order to determine if each permitted TNC is in compliance with Pub. Util. Code § 5445.2 and decide if additional background check requirements should be imposed.

Since allowing TNCs to operate in California, the Commission has issued permits to 13 TNCs that do not primarily transport minors: Ainos dba Witz, Altruistic, Inc. dba Bounce, Executive Ride, Quickie Technologies, Inc., Rasier-CA, Ride Plus, LLC, See Jane Go, Inc., Lyft, Silver Ride, LLC, Sitbaq, Inc., Social Drv, and Wingz. In addition, the Commission has issued permits to three TNCs that primarily transport minors: Kanga Do; Hop, Skip and Drive, and Zum. As part of the comment process, we have invited all parties to discuss the background-check issue, and to specifically opine on whether fingerprinting should be part of the checking process. Not all TNCs filed comments so the current state of the record does not permit the Commission to determine if all TNCs are in compliance with the newly enacted statutory background check requirements. As set forth in Ordering Paragraph 2, each licensed TNC will be required to file and serve a declaration in this proceeding attesting to how it complies with Pub. Util. Code § 5445.2 as well as the additional requirements adopted by this decision. The assigned Commissioner, the assigned Administrative Law Judge, and the Commission's TEB will have the discretion to determine if any follow-up inquiries are warranted regarding a

---

6 http://www.cpuc.ca.gov/uploadedFiles/CPUC_Public_Website/Content/Licensing/Transportation_Network_Companies/TNC%20Application%20Packet_Oct%202016.pdf.

TNC's background check program. New TNCs pursuing licensing after the effective date of this decision must include a similar attestation as part of their applications to the Commission's License Section.

While not every TNC filed comments regarding the current background check requirements, Rasier-CA and Lyft filed extensive comments on August 29, 2016 (which were later referenced in their comments filed on May 1, 2017)[7] regarding how they conduct their background checks of TNC drivers. We have chosen to take a closer look at the responses of these two TNCs, who comprise the majority of the TNC business market in California.[8] In doing so, the Commission can ascertain if the majority of TNC patrons are being transported by drivers whose backgrounds have undergone the screening scrutiny that California now requires. We can then compare the processes that Rasier-CA and Lyft utilize with the biometric background check program that the DOJ utilizes to determine if the Commission should add a biometric component to the background-checking process for all TNC drivers.

Rasier-CA and Lyft

Rasier-CA and Lyft perform similar background checks to identify drivers, search for personal information, and verify information accuracy, through contracting with the background check companies Checkr (Rasier-CA) and Sterling Talent Solutions (Lyft).[9]

---

[7] Lyft's May 1, 2017 Comments at 13 and footnote 29; *See* Rasier-CA's May 1, 2017 Comments at 8-9.

[8] We base this assessment of Rasier-CA and Lyft's market share based on the ride data provided to the Commission's Transportation and Enforcement Branch.

[9] Lyft's May 1, 2016 Comments at 17; and supporting Declaration of Kelly Kay (Kay Dec.) at 1, ¶ 3; Rasier-CA's May 1, 2016 Comments at 6; and supporting Declaration of Jared Callahan (Callahan Dec.), ¶ 5. Checkr and Sterling are credit reporting agencies (CRAs) audited and accredited by the Background Screening Credentialing Council (BSCC) of the National Association of Professional Background Screeners (NAPBS). Rasier-CA's May 1, 2017 Comments at 5, footnote 6, and 9; Callahan Dec. at ¶ 8; *Maryland Order* at 7, footnote 33; and 9-10, footnote 49. To pass an audit, a credit reporting agency must demonstrate continued compliance with a comprehensive set of accreditation standards, including (1) maintaining auditing procedures for quality assurance in regard to its active public record researchers; (2) maintaining procedures to assure maximum possible accuracy when determining the identity of an individual who is the subject of a record prior to reporting the information; (3) designating a qualified

Footnote continued on next page

The companies generally follow the following processes:

Step 1: Identify. TNC applications require prospective drivers to provide a basic set of personal data points, such as full name, photo, SSN, driver license number, date of birth, address, phone number, insurance information and vehicle information.[10]

Step 2: Search. Background check companies utilize application data to search for additional records associated with the driver-applicant.[11]

a. **Credit Check**. Sterling and Checkr utilize the applicant's name and SSN to obtain and review reports compiled by major credit bureaus to search for an applicant's other names and aliases, SSN, known addresses and periods of residence. The background checkers search for other data points if publicly available, such as property deeds, US Postal records or mail forwarding service, utility bills, voter's registration, and birth or death master files.[12]

b. **Photos.** Background companies also confirm an applicant's identity by comparing a current photo, typically a "selfie," against the current driver license photo.[13]

c. **Department of Motor Vehicle's (DMV's) Employer Pull Notice Program**. The California Public Utilities Commission (CPUC or Commission) requires TNCs to enroll in the DMV's Employer Pull Notice program, which permits the TNCs to review and receive close-in-time updates on a driver's driving records.[14]

d. **Database searches.** Both companies state they check publicly-available databases, which include:

---

individual(s) or position(s) within the organization responsible for understanding court terminology, as well as understanding the various jurisdictional court differences; and (4) having procedures in place to ensure the accuracy and quality of all work product. *See* NAPBS Background Screening Agency Accreditation Program: CRA Accreditation Standard with Audit Criteria (February 16, 2009) located at www.napbs.com. The criteria are also cited in the *Maryland Order* at 7, footnote 33; and 9-10, footnote 49.

[10] Callahan Dec. at ¶ 10; Kay Dec. at ¶ 4.

[11] Callahan Dec. at ¶ 9; Kay Dec. at ¶ 5.

[12] Callahan Dec. at ¶¶ 11-13; Kay Dec. at ¶ 8.

[13] Rasier-CA's Comments at 17; *see* Lyft's Comments at 21.

[14] Rasier-CA's Comments at 7 and footnote 23. Pub. Util. Code § 5444 requires TNCs to participate in the Pull-Notice System.

- U.S. Department of Justice Sex Offender Registry.[15]
- Interpol; Federal Bureau of Investigation (FBI) Terrorist Watch list; and Public Access to Court Electronic Records, a database maintained by the federal court system, which provides case records and outcomes from the 94 federal district courts.[16]

Step 3: Investigation. Many cities and counties make criminal records available to the public. Checkr and Sterling utilize an applicant's geographic locations to search for electronic and paper criminal records, and compile a list of offenses. Rasier states its background checks search approximately 1,500 national, state and local criminal databases that make such information public.[17]

Lyft utilizes three proprietary databases compiled by private companies:

- Social Security Number Trace database that contains hundreds of sources to locate known addresses, including information from all credit bureaus, property deeds/mortgages, U.S. Postal forwarding service and other public sources, e.g., voter registration. That screen provides locational data to determine which county/ies to search for the most up to date information regarding the applicant.[18]
- Enhanced Nationwide Criminal Search, which compiles thousands of publicly-available data sources, includes county criminal records, state repositories, state department of corrections records and national security databases.[19]
- Locator Select, which specifically searches public records from booking and incarceration locations for information regarding arrest dispositions and pending cases.[20]

Our review of these protocols leads us to conclude that Rasier-CA and Lyft are in compliance with Pub. Util. Code § 5445.2 (a)(1). Both Rasier-CA and Lyft contracted

[15] Callahan Dec. at ¶ 17; Kay Dec. at ¶ 7

[16] Callahan Dec. at ¶ 17; Kay Dec. at ¶ 7.

[17] Callahan Dec. at ¶ 16.

[18] Kay Dec. at ¶ 8.

[19] Kay Dec. at ¶ 13.

[20] Kay Dec. at ¶ 14.

with companies (Checkr and Sterling, respectively) that conduct searches of multistate and multi-jurisdiction criminal records locators or other similar commercial nationwide databases. Checkr and Sterling also conduct a search of the United States Department of Justice National Sex Offender Public Web site.

In addition, Checkr and Sterling are credit reporting agencies (CRAs) that are accredited and audited by the National Association of Professional Background Screeners (NAPBS). In order to pass the accreditation process, a CRA must comply with the requirements that NAPBS has established in the following fields: data information and security; legal and compliance; client education; research and data standards; verification and service standards; and miscellaneous business practices. In order to ensure consistent application of these standards, the Commission has determined that if a TNC wishes to employ a CRA to conduct background checks, or if the TNC itself wishes to conduct the background checks, the accreditation standards set by the NABPS must be met. As the accreditation standards are lengthy, we have appended them to this decision as Attachment A.

But given the importance of ensuring that background check process is as comprehensive, accurate, and secure as possible, we highlight below some of the accreditation standards:

> **Database Criminal Records**: When reporting potentially adverse criminal record information derived from a non-government owned or non-government sponsored/supported database pursuant to the federal Fair Credit Reporting Act, the CRA shall either: (a) verify the information directly with the venue that maintains the official record for that jurisdiction prior to reporting the adverse information to the client; or (b) send notice to the consumer at the time information is reported.
>
> **Auditing Procedures**: CRA shall maintain auditing procedures for quality assurance in regard to their active public record researchers.
>
> **Identification Confirmation**: CRA shall follow reasonable procedures to assure maximum possible accuracy when determining the identity of a consumer who is the subject of a record prior to reporting the information.

> CRA shall have procedures in place to notify client of any adverse information that is reported based on a name match only.
>
> **Jurisdictional Knowledge:** CRA shall designate a qualified individual(s) or position(s) within the organization responsible for understanding court terminology, as well as understanding the various jurisdictional court differences if CRA reports court records.
>
> **Verification Accuracy**: CRA shall maintain reasonable procedures to assure maximum possible accuracy when obtaining, recording and reporting verification information.
>
> **Data Security**: CRA shall have procedures in place to protect consumer information under the control of the CRA from internal and external unauthorized access. These procedures shall include specifications for the securing of information in both hard copy and electronic form, including information stored on portable and/or removable electronic devices.

With respect to Pub. Util. Code § 5445.2 (a)(2) and (3), a number of the offenses set forth therein that would disqualify a person from becoming a TNC driver (*e.g.* conviction of a violent felony or a violent crime, driving under the influence of drugs or alcohol) are similar to the disqualifying categories that the Commission articulated in Ordering Paragraph 4 of D.13-09-045, which states in part:

> Any felony criminal conviction within seven years prior to the date of the background check for driving under the influence of drugs or alcohol, fraud, use of a motor vehicle to commit a felony, a violent crime or act of terror, a sexual offense, a crime involving property damage, and/or theft will make the applicant ineligible to be a TNC driver.

Thus, all TNCs have been under a duty since 2013 not to hire a person as a TNC driver if he/she has been convicted of any of the above disqualifying convictions within the prior seven years.

As for remaining disqualifying convictions set out in Pub. Util. Code § 5445.2 (a)(2) and (3) (*e.g.* violation of Penal Code §§ 11413, 11418, 11418.5, or 11419; Election Code § 18540; or Penal Code §§ 67, 68, 85, 86, 92, 93, 137, 138, 165, 518, 530, 18500, 484(a), 487(a), or 25540(b)), we will require Rasier-CA, Lyft, and all

other TNCs to certify by declaration that they do not contract with, employ, or retain a driver that falls within any of these disqualifying categories.

1.5. Biometric Background Checks Performed by the California Department of Justice

Biometric background checks have been employed for decades as an integral part of the process for reviewing the suitability of prospective employees.[21] According to the State of California Office of the Attorney General's fact sheet entitled FINGERPRINT BACKGROUND CHECK,[22] the DOJ is required to maintain a statewide criminal record repository,[23] and uses this information to compile records of arrest and prosecution, known as Record of Arrest and Prosecution (RAP) sheets. The DOJ disseminates the information for law enforcement and regulatory (*i.e.* employment and licensing) purposes.[24] These RAP sheets are based on fingerprint submissions, "and therefore positively identified biometrically: a process by which a person's unique identity is confirmed."[25]

---

[21] *See The Attorney General's Report on Criminal History Background Checks* (June 2006): "There is widespread interest in obtaining access to criminal history record information from reliable sources for the purpose of screening an individual's suitability for employment, licensing, or placement in positions of trust." Further: "Fingerprint identification has been a major responsibility of the FBI since 1924 and fingerprints have been a key part of the FBI's national criminal history record system." (At 1 and 14.) Pursuant to Rule 13.9, the Commission takes Official Notice of this report pursuant to Evidence Code § 452.

[22] https://oag.ca.gov/fingerprints. Pursuant to Rule 13.9, the Commission takes Official Notice of this fact sheet pursuant to Evidence Code § 452.

[23] This claim is confirmed by Penal Code § 11105(a)(1): "The Department of Justice shall maintain state summary criminal history information." State summary criminal history is defined as "the master record of information compiled by the Attorney General pertaining to the identification and criminal history of a person, such as name, date of birth, physical description, fingerprints, photographs, dates, of arrests, arresting agencies and booking numbers, charge, dispositions, and similar data about the person." (Penal Code § 11105 (a)(2)(A).)

[24] Pursuant to Penal Code § 11105(b): "The Attorney General shall furnish state summary criminal history information to any of the following, if needed in the course of their duties…."

[25] https://oag.ca.gov/fingerprints.

The Penal Code also contains a protocol for the dissemination of criminal records. Criminal offender record information (sometimes referred to as CORI) is defined as "records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release." (Penal Code § 11075(a).) Pursuant to Penal Code § 11076, CORI may only be disseminated to agencies authorized by statute to receive such information. Pursuant to the DOJ fact sheet, the background check process is as follows:

> **Step 1. DOJ Fingerprint-Based Process.** First, an applicant visits a Livescan location. Livescan sites require an applicant to provide an identity verification document, which does not need to include a photo of the applicant. Such documents are collected along with the applicant's fingerprints, by employees trained and certified to "roll" fingerprints and who have themselves undergone a background check.
>
> **Step 2. Livescan transmittal.** Livescan will automatically transmit the images to the DOJ fingerprint database. Information transmitted to DOJ is searched against all other fingerprint in its database. If a match is identified, the individual's record is reviewed by a DOJ technician to assess the individual's criminal history, and determine whether the individual's information can be disseminated to the requesting agency (which must be statutorily authorized to receive the information). Based on these searches, the individual's record is returned from the California DOJ to the requesting agency with either a "no record" response or a "delay notice," indicating that manual review is underway. The no record/delay notice response is sent to the requesting agency within 48 to 72 hours of the fingerprint submission via Livescan.
>
> **Step 3. Research and Verification**. DOJ staff researches each open arrest record that lacks associated criminal history and/or a disposition. Its staff will make a "genuine effort" mandated by statute and case law, which consists of contacting arresting agencies, District Attorney, court or probation offices to determine disposition of that arrest.[26] Some entities

[26] Xavier Becerra, California Attorney General. *Fingerprint Background Checks*. https://oag.ca.gov/fingerprints. Pursuant to Rule 13.9 and Evidence Code § 452, the Commission takes

Footnote continued on next page

> allow DOJ to connect directly to local public or non-public case management systems; otherwise DOJ contacts the entity and receives the information by phone or fax.[27] Once the "genuine effort" is fulfilled, the criminal history record is updated, the RAP sheet is reviewed again, and the background check response is prepared and sent to the applicant agency.[28]

A statutory mandate allows DOJ to provide the information it possesses only to those authorized to receive it. (Penal Code § 11105.) Information provided includes, but is not limited to, all convictions and sex offender status. DOJ will not disseminate information regarding an arrest that lacks follow up information or a final disposition, typically those made over 20 years ago.

DOJ follows the same process if a California agency requests a federal fingerprint background check.[29] The DOJ forwards the fingerprint images to the FBI to perform a fingerprint-based search of records in the FBI's national criminal history database.[30] If the applicant's fingerprints match fingerprints in the national criminal history database, the FBI sends the DOJ a cumulative RAP sheet that contains criminal history information from any states or federal agencies that have reported the information to the FBI.[31] If there is not a matching disposition for every out-of-state or federal arrest, the DOJ must again perform the "genuine effort" to obtain the missing disposition information. Once the "genuine effort" is fulfilled, a DOJ technician must review the updated RAP sheet and prepare the background check response.[32]

---

official notice of the information from the Attorney General's website regarding the Department of Justice's fingerprint background checks.

[27] *Id*.

[28] *Id*.

[29] *Id*.

[30] *Id*.

[31] *Id*.

[32] *Id*.

Federal law precludes the DOJ from disseminating federal criminal history information to non-governmental entities.[33] Such entities receive a "fitness determination" from DOJ.[34]

Under Penal Code § 11105.2, the DOJ may provide subsequent state or federal arrest or disposition notice to any entity authorized by state or federal law to receive state or federal summary criminal history information upon the arrest or disposition of any person whose fingerprints are maintained at DOJ or the FBI as the result of an application for licensing, employment, certification or approval. The statute also defines certain terms and criteria. Relevant terms include "Need to Know," which is the necessity to obtain CORI in order to execute official responsibilities; and "Right to Know," the right to obtain CORI pursuant to a court order, statute or decisional law.

Penal Code § 11102.2 requires every authorized agency to designate at least one Custodian of Record responsible for the security, storage, dissemination, and destruction of the criminal records furnished to the agency and who serves as the primary contact for DOJ for any related issues.

1.6. AB 1289 and the Commission's Authority to Interpret, Enforce, and Adopt Additional Background Requirements

While the Commission set out questions related to biometrics within background checks in two ruling, the Legislature in 2016 articulated a scope and process for background checks for TNC drivers. On September 28, 2016, Governor Brown approved AB 1289,[35] which added § 5445.2 to the Pub. Util. Code, and required TNCs to conduct the following criminal background checks on TNC drivers:

---

[33] *Id*. "Access to criminal history summary records maintained by the DOJ is restricted by law to legitimate law enforcement purposes and authorized applicant agencies."

[34] California Department of Justice, Bureau of Criminal Information and Analysis Applicant Record & Certification Branch. Christina Rogers, Assistant Bureau Chief. February 17, 2017.

[35] Stats 2016, Ch. 740.

Pub. Util. Code §	**Topics: Requirements for Background Checks/Restrictions on TNC driver hiring, contracting, and retention**	**Text of Statute**
5445.2(a)(1)	Scope of required minimum background check that TNC or a third party must perform	Multistate and multijurisdiction criminal records locator or other similar commercial nationwide database with validation (5445.2(a)(1)(A)); and Search of United States Department of Justice National Sex Offender Public Web site (5445.2(a)(1)(B))
5445.2(a)(2)	A TNC may not contract with, employ, or retain persons	Currently registered on the DOJ National Sex Offender Public Web site (5445.2(a)(2)(A)); Convicted of either a violent felony or a violation of Penal Code §§ 11413, 11418, 11418.5, or 11419 (5445.2(a)(2)(B))
5445.2(a)(3)	A TNC may not contract with, employ, or retain persons convicted of any of the following offenses within the previous seven years	Misdemeanor assault or battery (5445.2(a)(3)(A)); Domestic violence offense (5445.2(a)(3)(B)); Driving under the influence of alcohol or drugs (5445.2(a)(3)(C)); A felony violation of Elections Code § 18540, or Penal Code §§ 67, 68, 85, 86, 92, 93, 137, 138, 165, 518, 530, 18500, 484(a), 487(a), or 25540(b) (5445.2(a)(3)(C))

By adding Pub. Util. Code § 5445.2(a)(5), the Legislature made it clear that the above requirements were *minimum* standards, since nothing in the statute should be interpreted to prevent a TNC from imposing additional background check standards. Similarly, pursuant to Pub. Util. Code § 5441, this Commission is also free to require

additional background checks as long as the Commission acts in a manner consistent with Article 7 (regulations for Transportation Network Companies [5430-5445.2] of the Pub. Util. Code. As newly enacted Pub. Util. Code § 5445.2 is part of Article 7, the Commission has the legislatively-granted authority to exercise its rulemaking power and require that TNCs conduct searches of additional information databases that could have information bearing on the suitability of an existing or prospective TNC driver.

Even without Pub. Util. Code § 5441, the Commission would be within its authority to interpret and, if necessary, require TNCs to adopt additional background-check requirements. The Commission is a state agency of constitutional origin whose power to establish rules has been liberally construed. (*So. Cal. Edison Co v. Peevey* (2003) 31 Cal.4th 781, 792; and Cal. Const., Art. XII, § 4 [The Commission "may fix rates and establish rules for the transportation of passengers…by transportation companies"].) The grant of authority over transportation companies was extended to charter-party carriers with the 1961 enactment of the Charter-Party Carriers of Passengers Act, which added Pub. Util. Code §§ 5251-5444. Later, with D.13-09-045, this Commission determined that TNCs were a category of charter-party carriers over which this Commission had jurisdiction, a decision the Legislature recognized when it enacted Pub. Util. Code §§ 5430-5444. Of particular note is Pub. Util. Code § 5440 (a), which states:

> The commission has initiated regulation of transportation network companies as a new category of charter-party carriers and continues to develop appropriate regulations for this new service.

Pursuant to Pub. Util. Code § 5381:

> To the extent that such is not inconsistent with the provisions of this chapter, the commission may supervise and regulate every charter-party carrier of passengers in the State any may do all things, whether specifically designated in this part, or in addition thereto, which are necessary and convenient in the exercise of such power and jurisdiction.

By extension, the Commission's broad authority granted by the California Constitution and by Pub. Util. Code § 5381 to regulate charter-party carriers and to do all things whether specifically designated or not, would include the ability to interpret and apply the TNC background-check provision found in Pub. Util. Code § 5445.2.

2. Discussion

The Commission received numerous Comments and Reply Comments from parties, as well as 1,817 responses from the public in online comments as of July 19, 2017. The general position taken by the parties aligns with one of two viewpoints—support or opposition for requiring fingerprint-based background checks of all existing and prospective TNC drivers. Those Parties supporting fingerprint-based background checks include the SFTWA, LADOT, SFO, and the SFMTA. HopSkipDrive also supports background checks but for all TNCs, not just those that primarily focus on transporting unaccompanied minors. Opposition to the fingerprint requirement comes from the two major TNCs, Rasier and Lyft. Further discussion herein will at times refer generally to these parties as proponents or opponents. As noted above, among the public survey responses submitted, 48% support requiring fingerprint-based background checks, 49% oppose, and about 2% are undecided.

2.1. Question 1: What Public Policy and/or Safety Objectives Would be Achieved by Requiring All Existing and Prospective TNC Drivers to Undergo a Biometric (i.e. the Use of a Person's Physical Characteristics and Other Traits) Background Check?

2.1.1. Party Comments

The supporters of fingerprint-based background checks strongly argue this requirement will improve rider safety, arguing that it is a reliable and effective means of

screening drivers.[36] They state that only fingerprinting can positively identify a driver-applicant,[37] whereas the currently required commercial background checks are susceptible to applicants using an alias or changed SSN.[38] Furthermore, these parties drew attention to a case where the San Francisco and Los Angeles District Attorney alleged over twenty Uber drivers that had passed the company's background check had a disqualifying criminal record.[39] However, this 2014 claim of unlawful and fraudulent business practices relating to the company's safety representations ultimately settled, resulting in neither confirmation nor refutation of the allegations.[40]

In contrast, Rasier and Lyft set forth a number of negative outcomes that could occur if the Commission adopted a biometric-based background check requirement: first, it is a myth that scanned fingerprint matching is infallible since both false positive and false negatives can occur with fingerprint matching.[41] As support, Lyft cites to the California Attorney General's website for the proposition that poor fingerprint quality impacts the system's ability to confirm or dismiss a potential fingerprint match.[42] Lyft also cites to a warning from the FBI about the increasing incidence of individuals altering their fingerprints to fool the FBI's Automated Fingerprint Identification System.[43] Second, Rasier-CA argues that criminal databases may be incomplete because a criminal

---

[36] Opening Comments of SFTWA at 1, May 1, 2017.

[37] Opening Comments of SFO and SFMTA at 1, May 1, 2017.

[38] Opening Comments of LADOT at 1, May 1, 2017.

[39] Opening Comments of SFTWA at 2; Opening Comments of SFO and SFMTA at 2; Opening Comments of LADOT at 2.

[40] Opening Comments of SFTWA at 2.

[41] Opening Comments of Lyft at 15. The Automated Fingerprint Identification System is a national fingerprint and criminal history system that is maintained by the FBI's Criminal Justice Information Services Division. (*The Integrated Automated Fingerprint Identification System*. U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division.)

[42] *Id.*

[43] *Id*.

history record can be triggered by a citation or other event where a fingerprint is not taken, and because there are some situations where fingerprints are not always taken at arrest.[44] If either of these situations occurs, the criminal history event will not appear in the repository.

The TNCs also assert that even if safety benefits exist, they do not outweigh the harm of a fingerprint requirement.[45] The flaws that the TNCs' claim are inherent in the fingerprint-based criminal history reports unfairly disadvantage all individuals seeking economic opportunities, especially minority populations.[46] Citing a series of historical and statistical studies, Rasier-CA argues that states have difficulty properly linking the arrest records with disposition information.[47] As African Americans are arrested at rates greater than their representation in the general population, the lack of complete disposition information, combined with the arrest incidents of persons of color, can result in certain racial groups being denied an employment opportunity as a TNC driver.[48] Thus, Rasier-CA and Lyft show skepticism for the practice of fingerprinting generally, especially as a means of determining whether an employment contracting opportunity should be offered to an individual.[49]

Additionally, Rasier-CA and Lyft assert that potential harm comes from inefficiencies and economic concerns. TNCs fear delay in receiving the background check results due to already overburdened government agencies needing to complete

[44] Opening Comments of Rasier-CA at 5.

[45] Opening Comments of Lyft at 14; Opening Comments of Rasier at 4, May 1, 2017.

[46] Opening Comments of Rasier-CA at 23.

[47] Opening Comments of Rasier-CA at 5.

[48] Opening Comments of Rasier-CA at 24.

[49] Opening Comments of Lyft at 14-17; Reply Comments of Rasier at 5-7, May 15, 2017.

arrest dispositions, as well as from processing fingerprints.[50] Rasier-CA believes its current background check is more efficient and thus reduces these concerns.[51]

Further, Rasier-CA draws on the *Maryland Order* as support for the view that commercial background checks can meet safety standards just as well as fingerprint-based government checks drawing on law enforcement databases.[52] Maryland's PSC describes Rasier's commercial background checks as being "as comprehensive and accurate as the government fingerprint-based background check process."[53]

2.1.2. Discussion

After weighing the respective merits of each side's position, the Commission declines at this time to add a biometric-based background requirement to those in Pub. Util. Code § 5445.2. The Commission finds that the commercial background checks currently employed by Rasier and Lyft are compliant with the standards imposed by Pub. Util. Code § 5445.2. Although we recognize the public's familiarity with fingerprinting, we do not see that a demonstratively greater level of safety would be added over and above the current background-check protocols. As the record shows, individuals submitting fingerprints via Livescan are not required to use a photo I.D. to establish their identity at the Livescan site. In addition, law enforcement agencies themselves have acknowledged that the quality of their records is only as accurate and up-to-date as the information provided by local courts and law enforcement agencies. When errors exist in criminal justice records or resource shortages lengthen the time required for final case dispositions, the time required for a DOJ technician to resolve an individual's fingerprint can contribute to a lengthy delay in determining their eligibility for employment. In

[50] Opening Comments of Rasier at 5-6.

[51] *Id.* at 8.

[52] *Id.* at 4-5.

[53] *Id.* at 5.

contrast, with the standards set by the Legislature in Pub. Util. Code § 5445.2 and documentation to be submitted to the Commission by each TNC consistent with this decision, the drawbacks of a fingerprint-based background check can be avoided, while still ensuring public safety. In sum, allowing a process that includes commercial background checks, presented to the Commission's TEB via attestation with supporting documentation and subject to staff review and verification, satisfies the Commission's public policy and safety objectives, and allows flexibility to meet the background requirements that the Legislature has mandated.

In deciding not to add a biometric background requirement, we are in no way endorsing the argument that it is inappropriate for the Commission to require fingerprint-based background checks. Lyft believes that because the Legislature had the opportunity to require fingerprint-based background checks, but chose not to, the Commission is preempted from setting this standard. But for the reasons set forth above at Section 1.6, this argument has no merit, as it would be contrary to the Commission's expressed grant of authority to interpret and enforce laws affecting its ability to regulate those entities that are subject to the Commission's jurisdiction.

2.2. Question 2: Does Subjecting All TNC Drivers to a Biometric Background Check Adversely Affect the Chances of Persons of Different Races or Ethnicities to Pass the Background-Checking Process?

2.2.1. Party Comments

There is a distinct split in opinions among the proponents and opponents of fingerprint-based background checks regarding impact on racial and ethnic groups. As discussed above in Section 2.1.1., the TNCs believe requiring fingerprint-based background checks will disparately impact some minority groups, stemming from the potential delay in receiving fingerprint-based background checks from government agencies.

The proponents of fingerprinting do not share this same concern. Although they acknowledge the problem of disproportionate arrests among certain minority groups,[54] they believe current California laws adequately protect these minority groups during the hiring process. The proponents point to laws such as 11 C.C.R. § 721-24, that prevent the dissemination of arrest records without a complete arrest disposition. This keeps people who were unfairly arrested from having such arrests without disposition reported. The fingerprint-based background check proponents add support to their argument by noting the large number of minorities currently employed in their localities as taxi drivers.[55] They say this shows fingerprint-based background checks have not limited people of different races and ethnicities from getting hired to drive.

TNCs counter the proponents by saying that the prohibition against dissemination of incomplete arrest records is exactly the cause of their concern—that it creates unfair delay.[56] The concern is not that fingerprinting will allow TNCs to reject applicants based on incomplete arrest dispositions, but that the process of completing arrest dispositions means certain minority groups are disproportionately forced to wait. This argument accepts the protections provided by California law, but denies that the law or anything else can reduce the delay that certain minority groups will disproportionately face.

Additionally, TNCs rebut the worth of the fact that a large number of taxi drivers are from minority groups.[57] In their view, showing the number of employed drivers does not enlighten the issue of delays in hiring. Nor does it show that these minorities are from groups subject to disproportionate arrests. Rasier's Reply Comments claim the

[54] Opening Comments of LADOT at 3; Opening Comments of SFTWA at 5; Opening Comments of SFO and SFMTA at 4.

[55] Opening Comments of LADOT at 3.

[56] Reply Comments of Rasier at 7.

[57] *Id.* at 7-8.

proponents point here ". . . reveal[s] nothing about the racial impact of a fingerprint-based background check . . ."[58]

2.2.2. Discussion

The record developed to date does not permit the Commission to make a determination one way or another about the claimed discriminatory impact of biometric checks on minority TNC driver applicants. While we are concerned about the potential disparate impact that could be felt by minority groups that may face disproportionate arrests levels and the criminal justice system's slow process – or failure – to achieve disposition of the arrests, our decision today is based on the showing by some of the TNCs that the background check processes they currently use meet the safety concerns of the Commission without a biometric background component. The Commission does, however, reserve the right to study this question further.

2.3. Question 3: In Addition to a Biometric Background Check, Are There Other Background Check Protocols that the Commission Should Consider Adopting?

In answering Question 3, the parties combined their responses so that they are equally applicable to Questions 4[59] and 5.[60] The Commission will do the same with its response.

2.3.1. Comments

Some comments focused on facilitating a two-tiered system[61] incorporating both fingerprint-based and commercial background checks. These points will not be as

---

[58] *Id.* at 8.

[59] How Would Any Other Background Check Protocols Described in Question 3 Above Satisfy California's Public Policy and/or Safety Objectives?

[60] What Background Check Protocol Should the Commission Adopt to Comply with the Requirements and Goals of Assembly Bill 1290, Codified at Public Utilities Code Section 5445.2?

relevant to our discussion here since we have decided not to implement a fingerprint-based background check standard. For that reason, reference to the proponents' discussion of a two-tiered system will not be included.

The TNCs provided a variety of suggestions for potential additional requirements to the current commercial background check standard. Both Rasier and Lyft suggested we permit only commercial background check companies that have been audited and accredited.[62] They name the National Association of Professional Background Screeners[63] (NAPBS) as such a group that could audit and accredit companies that perform background checks. Additionally, Rasier and Lyft seek clarification of any Commission rules and regulations that may conflict with or relate to Public Utilities Code Section 5445.2,[64] as well as definitions of terms in that code section.[65]

Lyft made some further proposals that Rasier did not. These include the requirement that TNCs verify applicant identity by reference to a California driver license[66] and that TNCs conduct annual background checks.[67] The license requirement for the application process provides a positive identification of the driver, while not being overly burdensome because a driver license is already an application requirement. It simply incorporates the license into the background check phase of hiring. The annual background check requirement is an idea that comes from Lyft's current business practice. Lyft runs a background check on the anniversary of each driver's approval to

---

[61] Opening Comments of SFTWA at 6; Opening Comments of LADOT at 3; Opening Comments of SFO and SFMTA at 6.

[62] Opening Comments of Rasier at 12; Opening Comments of Lyft at 10.

[63] *See generally* National Association of Professional Background Screeners, https://www.napbs.com/. (last visited July 31, 2017).

[64] Opening Comments of Rasier at 12.

[65] Opening Comments of Lyft at 9.

[66] *Id.* at 13.

[67] *Id.*

operate on the Lyft platform. They claim that the Commission could make this a requirement of all TNCs to help further the Commission's safety objectives.

For proponents of fingerprint-based government background checks, there were only a few suggestions made that did not necessarily incorporate the fingerprint standard. All such suggestions came from SFTWA. Their suggestions include use of the Trustline Registry[68] and limiting commercial background checks to only revealing those crimes that would disqualify the driver.[69] The Trustline Registry was suggested in combination with a fingerprint-based check, but the proposal could also be implemented without fingerprint-based background checks. The suggestion to limit searchable background information comes from SFTWA's fear of abuse by TNCs. SFTWA claims abuse could occur with the current background check system because TNCs can receive a wealth of background information that is beyond the information relevant to disqualifying offenses. SFTWA does not cite any occurrences of this, but believes it could easily happen.

2.3.2. Discussion

Questions three through five generally sought comments on what further measures to take for TNC background check requirements, how those measures improve safety, and how they relate to AB 1289. The parties all returned thoughtful proposals, some of which will be adopted in some variation. Other proposals were well-taken and considered, and will be kept in discussion by the Commission moving forward as we continue to promote safety. Policies that this Commission adopts today are as follows:

> First, if a TNC uses a commercial background check company to conduct background checks of its driver applicants, the company must be accredited by the NAPBS BSCC and must comply with the audit and accreditation

[68] Opening Comments of SFTWA at 6. The Trustline Registry is California's database of providers of care to minors, in which the provider has cleared a criminal background check, including fingerprinting. The Commission requires TNCs that primarily transport minors to use the Trustline Registry for their drivers. D.16-04-041.

[69] *Id.* at 7.

criteria discussed in Section 1.4 and Ordering Paragraph 2 of this decision. Commercial background check companies have the support of the California Legislature, as seen in Pub. Util. Code § 5445.2, and the Commission similarly finds that they have the ability to safely evaluate driver-applicants for TNCs. If a TNC conducts background checks in-house, then the TNC must be accredited by the NAPBS BSCC and must comply with the audit and accreditation criteria discussed in section 1.4 and Ordering Paragraph 2 of this decision.

Second, each TNC must receive proof of accreditation of the background check company and provide proof of accreditation with any reporting that the Commission may require. Such proof will be required of presently licensed TNCs within 30 days of this decision, and annually thereafter. Such proof will become part of the application process for new TNCs requesting a license to operate in California.

Third, the background screening for each TNC driver must be conducted prior to the granting of authorization to operate on the TNC's platform and repeated at least once per year thereafter, for as long as the TNC driver is authorized to operate on the TNC's platform.

Fourth, we limit the information a TNC can require from a background check to those disqualifying categories of offenses and convictions set forth in Pub. Util. Code § 5445.2. This protects applicants from any potential abuse, while not hampering the ability of TNCs to hire safe drivers.

3. Comments on Proposed Decision

The proposed decision of Commissioner Randolph in this matter was mailed to the parties in accordance with Section 311 of the Public Utilities Code and comments were allowed under Rule 14.3 of the Commission's Rules of Practice and Procedure. Opening comments were received from Rasier-CA, Lyft, SFMTA, SFTWA, and Dolan. Reply comments were received from Rasier-CA, Lyft, and SFTWA. We summarize the major points from the comments as follows:

Both Rasier-CA and Lyft recommend that the Commission remove the last bullet point from Ordering Paragraph 1 (the last bullet point states: "we limit the information a TNC can require from a background check to those disqualifying categories of offenses and convictions set forth in Pub. Util. Code § 5445.2.") on the grounds that it is unnecessary and inconsistent with state and federal law, and may impede their ability to

adjust their policies as needed. They stress the importance in having the flexibility to adjust their practices to changes in the criminal law to appropriately approve or disqualify a TNC driver applicant.

SFMTA, SFTWA, and Dolan question both the Commission's findings regarding the effectiveness of biometric background checks, as well as the conclusion not to require each TNC to add a biometric check component as part of the criminal background check of TNC drivers. They assert that a biometric background check will provide a more comprehensive criminal background screening than the process currently conducted by Rasier-CA and Lyft.

The Commission has considered the potential merits of each of these arguments, and has decided not to change the background check requirements except in one respect. With respect to the last bullet point in Ordering Paragraph 1, we add the word "criminal" before the word "background" so that the sentence reads as follows:

> We limit the information a TNC can require from a criminal background check to those disqualifying categories of offenses and convictions set forth in Pub. Util. Code § 5445.2.

That way, we clarify that a TNC may, in accordance with Pub. Util. Code § 5445.2(a)(5), impose additional standards. Additionally, some minor edits have been made.

4. Assignment of Proceeding

Liane M. Randolph is the assigned Commissioner and Robert M. Mason III is the assigned Administrative Law Judge in this proceeding.

Findings of Fact

1. Each TNC that responded in this proceeding performs similar background checks to identify drivers, search for personal information and verify information accuracy.

2. Rasier-CA and Lyft utilize background check companies Checkr and Sterling, respectively. Checkr and Sterling are CRAs audited and accredited by the BSCC of the NAPBS.

3. TNC applications require prospective drivers to provide a basic set of personal data points, such as full name, photo, SSN, driver license number, date of birth, address, phone number, insurance information and vehicle information.

4. Background check companies utilize application data to search for additional records associated with the driver-applicant.

5. Checkr and Sterling utilize an applicant's geographic location to search for electronic and paper criminal records, and compile a list of offenses.

6. Rasier-CA states its background checks search approximately 1500 national, state and local criminal databases that make such information public.

7. Lyft utilizes three databases compiled by private companies: Social Security Number Trace Database, Enhanced Nationwide Criminal Search, and Locator Select.

Conclusions of Law

1. Rasier-CA's background-check protocol complies with Publ. Util. Code § 5445.2.

2. Lyft's background-check protocol complies with Pub. Util. Code § 5445.2.

3. The background checks performed by Ainos dba Witz, Altruistic, Inc. dba Bounce, Executive Rides, Rasier-CA, Ride Plus, LLC, See Jane Go, Inc., Lyft, Silver Ride, LLC, Sitbaq, Inc., Social Drv, and Wingz presently comply with the requirements of D.13-09-045.

4. The background checks performed by Kanga Do; Hop Skip Drive; and Zum comply with the requirements of D.13-09-045 and D.16-04-041.

5. A TNC may conduct, on an in-house basis, the background checks for its participating and/or prospective drivers provided the TNC complies with Pub. Util. Code § 5445.2.

6. A TNC that is already permitted to operate in California, and elects to conduct the background checks on an in-house basis should satisfy all the requirements of Pub. Util. Code § 5445.2, as well as the additional requirements set forth in Ordering Paragraph 2 of this decision, and should file and serve a declaration of compliance with the

background check requirements no later than 30 days following the issuance of this decision.

7. A prospective transportation company that wishes to conduct, on an in-house basis, the background checks for its participating and/or prospective drivers should confirm with the Commission's Transportation Enforcement Branch, as part of the application process, that it will comply with the requirements of Pub. Util. Code § 5445.2, as well as the additional requirements set forth in Ordering Paragraph 2 of this decision.

8. All current and future TNC applicants should certify, as part of their applications, that their background check process complies with Pub. Util. Code § 5445.2, as well as the background check requirements set forth in Ordering Paragraphs 1 and 2 of this decision.

9. In addition to the requirements set forth in Pub. Util. Code § 5445.2, every licensed TNC should comply with the following additional requirements:

- First, commercial background check companies that a TNC employs must be accredited by the National Association of Professional Background Screener's BSCC.
- Second, each TNC must receive proof of accreditation of the background check company and provide proof of accreditation with any reporting that the Commission may require.
- Third, the background screening for each TNC driver will be conducted for each year the TNC driver subscribes to the app.
- Fourth, we limit the information a TNC can require from a criminal background check going past seven years to those disqualifying categories of offenses and convictions set forth in Pub. Util. Code § 5445.2. We do not limit the information a TNC can obtain regarding a TNC driver applicant within the previous seven years.

O R D E R

IT IS ORDERED that:

1. Any company wishing to provide Transportation Network Company (TNC) services in California shall satisfy the background-check requirements of Pub. Util. Code §5445.2 for its existing and prospective drivers:

   - A TNC or a third party working on the TNC's behalf must perform a search of multistate and multi-jurisdiction criminal records locator or other similar commercial nationwide database with validation; and conduct a search of the United States Department of Justice National Sex Offender Public Web site.
   - A TNC may not contract with, employ, or retain persons currently registered on the Department of Justice National Sex Offender Public Web site; or convicted of either a violent felony or a violation of Penal Code §§ 11413, 11418, 11418.5, or 11419.
   - A TNC may not contract with, employ, or retain persons convicted of any of the following offenses within the previous seven years: misdemeanor assault or battery; domestic violence offense; driving under the influence of alcohol or drugs; a felony violation of Elections Code § 18540, or Penal Code §§ 67, 68, 85, 86, 92, 93, 137, 138, 165, 518, 530, 18500, 484(a), 487(a), or 25540(b).

   In addition to the requirements set forth in Pub. Util. Code § 5445.2, every licensed TNC shall comply with the following additional requirements:

   - First, commercial background check companies that a TNC employs must be accredited by the National Association of Professional Background Screener's Background Screening Credentialing Council.
   - Second, each TNC must receive proof of accreditation of the background check company and provide proof of accreditation with any reporting that the Commission may require.
   - Third, the background screening for each TNC driver will be conducted for each year the TNC driver subscribes to the app.
   - Fourth, we limit the information a TNC can require from a criminal background check going past seven years to those disqualifying categories of offenses and convictions set forth in Pub. Util. Code §

5445.2. We do not limit the information a TNC can obtain regarding a TNC driver applicant within the previous seven years.

2. A criminal background check company (sometimes referred to as a credit reporting agency or CRA) that is retained by a Transportation Network Company must comply with the audit and accreditation standards that the National Association of Professional Background Screeners has adopted in the following fields: data information and security; legal and compliance; client education; research and data standards; verification and service standards; and miscellaneous business practices. These audit and accreditation standards, which are appended to this decision as Attachment A, include, but are not limited to, the following:

a. **Database Criminal Records**: When reporting potentially adverse criminal record information derived from a non-government owned or non-government sponsored/supported database pursuant to the federal Fair Credit Reporting Act, the CRA shall either: (a) verify the information directly with the venue that maintains the official record for that jurisdiction prior to reporting the adverse information to the client; or (b) send notice to the consumer at the time information is reported.

b. **Auditing Procedures**: CRA shall maintain auditing procedures for quality assurance in regard to their active public record researchers.

c. **Identification Confirmation**: CRA shall follow reasonable procedures to assure maximum possible accuracy when determining the identity of a consumer who is the subject of a record prior to reporting the information. CRA shall have procedures in place to notify client of any adverse information that is reported based on a name match only.

d. **Jurisdictional Knowledge:** CRA shall designate a qualified individual(s) or position(s) within the organization responsible for understanding court terminology, as well as understanding the various jurisdictional court differences if CRA reports court records.

e. **Verification Accuracy**: CRA shall maintain reasonable procedures to assure maximum possible accuracy when obtaining, recording and reporting verification information.

f. **Data Security**: CRA shall have procedures in place to protect consumer information under the control of the CRA from internal and external unauthorized access. These procedures shall include specifications for the securing of information in both hard copy and

electronic form, including information stored on portable and/or removable electronic devices.

3. Each Transportation Network Company (TNC) currently permitted to operate in California shall, within 30 days from the issuance of this decision, file and serve on the service list of this proceeding a declaration attesting to how it complies with Pub. Util. Code § 5445.2 as well as the additional requirements adopted by this decision. The assigned Commissioner, the assigned Administrative Law Judge, and the Commission's Transportation Enforcement Bureau will have the discretion to determine if any follow-up inquiries are warranted regarding a TNC's background-check program.

4. As an alternative to Ordering Paragraphs 1 and 2, a Transportation Network Company (TNC) may elect to conduct, on an in-house basis, its background checks for each driver, or a person who has applied to be a participating driver of the TNC. The in-house background check must comply with Pub. Util. Code § 5445.2, as well as the additional requirements set forth in Ordering Paragraph 2. A TNC that elects to conduct its background checks on an in-house basis shall file and serve a declaration of compliance with the background check requirements within 30 days from the issuance of this decision. As for a TNC that seeks authority to operate in California after the issuance of this decision and wishes to conduct its background checks on an in-house basis, the TNC must include a declaration of compliance as part of its TNC application that is submitted to the Commission's License Section.

5. Driver shall mean: a participating driver or driver who uses a vehicle in connection with a transportation network company's online-enabled application or platform to connect with passengers; or a person who has applied to be a participating driver of a transportation network company. A participating driver or driver shall carry proof of Transportation Network Company insurance coverage with him or her at all times during his or her use of a vehicle in connection with a transportation network company's online-enabled application or platform.

6. Rulemaking 12-12-011 remains open.

Dated _____, at San Francisco, California.

ATTACHMENT A

NAPBS - BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM **CRA ACCREDITATION STANDARD WITH AUDIT CRITERIA**

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
Data Information and Security		DEFINITION: Consumer information includes any information identifiable to one or more consumers, including that found in vendor reports, spreadsheets, consumer reports, paper or electronic information management systems, faxed documents, and client communications.	
1.1 Information Security			
CRA shall have a written information security policy. CRA shall designate one or more individuals within the organization who are responsible for implementing, managing and enforcing the information security policy.	CRA shall provide written information security policy.	CRA shall present written information security policy. If questioned, CRA employees should demonstrate knowledge of information security policy and be able to access current policy.	This is an overarching information security policy which broadly addresses security within the CRA environment. This policy may reference other security policies and/or procedures dealing with specific security topics. The security topics addressed may include some or all of the following, but are not limited to: confidentiality agreements with vendors and employees; physical security of consumer information; electronic security of consumer information; communicating consumer information to vendors, clients, and other parties; providing and communicating information to consumers; permissible uses of portable and/or removeable electronic storage devices.
	CRA shall employ or retain a minimum of one person who is responsible for CRA's overall information security program. This will be evidenced by written job description, policy, procedure, or other documentation. If various people are responsible for different aspects of the program, one person shall hold overall responsibility as evidenced by job description, organizational chart, or other documentation.	CRA shall present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for the overall information security program.	CRA shall make available documentation which clearly identifies person, by name and title, who is responsible for overall information security program.
1.2 Data Security			
CRA shall have procedures in place to protect consumer information under the control of the CRA from internal and external unauthorized access. These procedures shall include specifications for the securing of information in both hard copy and electronic form, including information stored on portable and/or removable electronic devices.	CRA shall provide written procedures in place to protect consumer information from unauthorized electronic and/or physical access. This includes the collection, use, storage, and destruction of consumer information in both paper and electronic form.	CRA employees dealing with consumer information shall be able to explain and demonstrate procedures for protecting consumer information in their posession, whether such information is used internally and/or externally, and be able to access current documentation. CRA will also be able to demonstrate electronic and physical protection of consumer information.	The policies and procedures designed to protect consumer information may include some or all of the following, but are not limited to: 1) securing unattended workstations, 2) limited access to networks, data, and work areas, 3) limiting consumer information provided to information sources to only that information which is needed to conduct a search, 4) destruction of hard copy documents, 5) identification of caller before providing consumer information, 6) employee badging or other identification system, 7) unescorted visitor policy, 8) secure document destruction, 9) secure transport of information, 10) use of encryption and/or secure networks and/or websites, 11) password assignment and replacement, 12) controlling use of portable storage devices, 13) alarm systems, 14) door locks, and 15) secure server and back-up sites.
1.3 Intrusion and Data Security			
CRA shall have procedures in place to detect, investigate and respond to an information system intrusion, including consumer notification where warranted.	CRA shall provide procedures for detecting and identifying information system intrusions (unauthorized access to computer systems and/or consumer data).	CRA shall make available the procedure, process, and/or tools used to monitor access and identify potential intrusions.	CRA should be able to present proof of tools used to protect network, data, and consumer information. This may be intrusion/detection testing results, firewall protections used, secure website, etc.

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
	CRA shall provide procedures for responding to information system intrusions including how consumer notification requirements are determined.	CRA shall make available the procedure, process, and/or tools used to respond to intrusions. If questioned, CRA employees should demonstrate knowledge of procedure to be followed in case of intrusion or suspected intrusion and be able to access current documentation.	Process/procedure should include some or all of, but is not limited to: 1) individual to contact in case of intrusion and his/her back-ups, 2) necessity of immediately stopping intrusion activity, if still occurring, 3) determination of notification requirements, 4) preparing notification, 5) obtaining necessary approvals of notification language, 6) communicating notification, and 7) de-brief to prevent future occurrences.
1.4 Stored Data Security			
CRA shall have procedures in place to ensure backup data is stored in an encrypted or otherwise protected manner.	CRA shall provide written policy, procedure or other documentation explaining data backup, storage, and access procedures.	CRA shall make available the individual responsible for data backup and storage. This individual shall be able to describe and/or provide documentation related to backup and data storage.	The process used to backup and store data should include: limiting backup to select authorized individuals, secure transport of backup tapes to storage facility, and security at the storage location. At a minimum this includes locked storage facility and password protected access.
1.5 Password Protocol			
CRA shall require strong password protocol pursuant to current security best practices.	CRA shall provide written policy, procedure, or other documentation which explains password protocol and how such protocol is used.	CRA shall make available the individual responsible for password protocol. This individual shall be able to describe and/or provide documentation related to password characteristics, assignment, replacement, and recordkeeping. If questioned, CRA employees who use passwords shall explain process to obtain a password for him/herself and/or client and be able to access current documentation.	CRA should demonstrate that password is required for sign-on and also demonstrate procedure for changing password. Required password should be a minimum of six (6) characters, preferably using both alpha and numeric characters. Records of password issuance should be securely maintained. A biometric solution would also be acceptable.
1.6 Electronic Access Control			
CRA shall have procedures in place to control access to all electronic information systems and electronic media that contain consumer information. CRA shall have procedures in place to administer access rights. Users shall only be given the access necessary to perform their required functions. Access rights shall be updated based on personnel or system changes.	CRA shall provide written policy, procedure or other documentation explaining how access rights to consumer information are controlled, administered, and limited.	CRA shall make available the individual responsible for controlling access to consumer information. This individual shall be able to describe and/or provide documentation and/or provide a demonstration related to access control. If questioned, CRA employees who receive such requests will demonstrate knowledge of process if change in access rights is to be requested.	Process should include some or all of, but is not limited to: 1) how users apply for and receive access, 2) authorization needed for access, 3) access parameters, 4) password issuance/replacement/expiration, 5) monitoring tools, and 6) recordkeeping.
1.7 Physical Security			
CRA shall have procedures in place to control physical access to all areas of CRA facilities that contain consumer information.	CRA shall provide written policy, procedure or other documentation explaining how access to areas of CRA facilities containing consumer information is controlled.	CRA shall provide auditor a tour of the facility, demonstrating and describing the physical security measures in place. Auditor may interview CRA staff about physical security procedures.	Process/procedure should include some or all of, but is not limited to, the following: 1) procedures for granting levels of access to CRA personnel (e.g., assignment of keys or security system passcodes), 2) procedures for authorizing and monitoring guests (including the auditor) to the facility, and 3) control of access by staff, contingent workers, vendors, etc.
1.8 Consumer Information Privacy Policy			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall have a Consumer Information Privacy Policy detailing the purpose of the collection of consumer information, the intended use, and how the information will be shared, stored and destroyed. The CRA shall post this policy on its Web site, if it has one, and will make said policy available to clients and/or consumers upon request in at least one other format.	CRA shall provide a copy of the Consumer Information Privacy Policy along with the address of the policy on the CRA's website (if CRA has website) and an explanation of other means by which privacy policy is communicated.	CRA employees shall be able to access current copy of Privacy Policy and describe process by which privacy policy may be communicated externally.	The policy should include some or all of, but is not limited to, the following: the purpose of the collection of consumer information, the intended use, and how the information will be shared, stored and destroyed. The CRA shall post this policy on its website, if it has one, and will make said policy available to clients and/or consumers upon request utilizing at least one other method.
1.9 Unauthorized Browsing			
CRA shall have a policy that prohibits workers from searching files and databases unless they have a bona fide business necessity.	CRA shall provide written policy, procedure, or other document (employee handbook, etc.) which instructs CRA employees on appropriate and/or inappropriate use of consumer information.	CRA employees with access to consumer information shall demonstrate knowledge of proper use of consumer information and be able to access current copy of documentation.	Documentation should include statement of appropriate use as being limited to business purposes only and include prohibition of browsing
1.10 Record Destruction			
When records are to be destroyed or disposed of, CRA shall follow FTC regulations and take measures to ensure that all such records and data are destroyed and unrecoverable.	CRA shall provide written policy, procedure, or other document (employee handbook, etc.) which instructs CRA employees on appropriate document destruction procedures.	CRA employees shall demonstrate knowledge and use of proper document destruction procedures and be able to access current documentation.	Documentation should require all consumer and client information be disposed of securely as to render information inaccessible, unreadable, and/or unrecoverable per current FTC rules in which the following methods are permitted: 1) burning, pulverizing, or shredding, 2) destroy or erase electronic files, and/or 3) after conducting due diligence, hire a document destruction company. In addition, paper documents containing personally identifiable information (particularly name, date of birth, and SSN) , if retained at individual desks/workstations, shall be destroyed or inaccessible no later than the end of each work day.
1.11 Consumer Disputes			
CRA shall have procedures in place for handling and documenting a consumer dispute that comply with the federal FCRA.	CRA shall provide written policy, procedure, or other documentation which instructs CRA employees on consumer dispute procedures.	CRA employees responsible for consumer disputes shall demonstrate knowledge of proper consumer dispute procedures and be able to access current copy of documentation. Auditor may request to see a (redacted) copy of dispute documentation.	The policies and procedures designed to handle consumer disputes must meet FCRA requirements which include, but are not limited to: 1) no charge to consumer; 2) re-investigate, correct, and/or delete disputed information within 30 days (or 45 days if extended) of notice of dispute; 3) notify information provider of dispute within 5 days of receipt; 4) consider information provided by consumer, 5) advise consumer if dispute is deemed frivolous or irrelevant 6) notify appropriate parties of dispute results, and 7) comply with consumer request for description of re-investigation process. In addition, CRA should document: 1) responsibility of CRA employee receiving consumer dispute, 2) how incoming consumer dispute letters/emails/phone calls should be routed upon receipt, 3) re-investigation responsibility and/or procedures, 4) process for updating/correcting consumer report, 5) recordkeeping, and 6) procedure to help prevent future occurrences (such as recommendation for training, software change, etc.)
1.12 Sensitive Data Masking			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall have a procedure to suppress or truncate Social Security numbers and other sensitive data elements as required by law.	CRA shall provide written policy, procedure, or other documentation describing suppression, truncation, or other methods used to protect and limit exposure of SSN's and other sensitive data elements as required by law.	CRA employees shall demonstrate knowledge of proper procedures for use of SSN's and other sensitive data elements as required by law and CRA employees shall be able to access current documentation. If interviewed, CRA employees shall demonstrate understanding of proper use and protection of SSN's and other sensitive data elements as required by law **AND if applicable**, the use of technology to protect SSN's and other sensitive data elements as required by law.	Documentation should include but is not limited to: 1) No more than the final four digits of SSN's shall be communicated in any form outside CRA employees unless an approved exception exists, 2) When use of SSN and other sensitive data elements as required by law is needed internally or externally, the data exposed shall be limited to only that which is needed for the specific business purpose which has been identified, 3) When communicating SSN's or other data elements as required by law outside the CRA environment, secure transport methods shall be used.
1.13 Database Criminal Records			
When reporting potentially adverse criminal record information derived from a non-government owned or non-government sponsored/supported database pursuant to the federal FCRA, the CRA shall either: A) verify the information directly with the venue that maintains the official record for that jurisdiction prior to reporting the adverse information to the client; or B) send notice to the consumer at the time information is reported.	CRA shall provide written policy, procedure, or other documentation describing method/s used to comply with current FCRA requirements of source verification or sending notice to the consumer at the time information is reported.	CRA employees responsible for the use of non-governmental criminal record databases shall demonstrate knowledge of compliant database reporting and be able to access current documentation.	The policy/procedure should include either: 1) process for verification of database information by researching in the originating jurisdiction/venue, or 2) process to inform applicant of potentially adverse information being reported to employer/prospective employer.
Legal and Compliance			
2.1 Designated Compliance Person(s)			
The CRA shall designate an individual(s) or position(s) within the organization responsible for CRA's compliance with all sections of the federal FCRA that pertain to the consumer reports provided by the CRA for employment purposes.	CRA shall employ a minimum of one person who is responsible for CRA's development, implementation, and on-going compliance with all applicable sections of the FCRA as evidenced by written job description/s or other documentation. If multiple people are responsible, one person shall hold CRA Leadership role and overall responsibility as evidenced by written job description or other documentation.	CRA shall present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for FCRA compliance. CRA shall make this person available either in person, by phone **OR** shall provide a signed affadavit or similar document in which the person has affirmed their responsibility for FCRA compliance within the organization. If interviewed, CRA employees shall identify the person/s who can provide FCRA expertise when needed.	Compliance CRA Leader shall affirm his/her role as being responsible for FCRA compliance within the organization.
2.2 State Consumer Reporting Laws			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
The CRA shall designate an individual(s) or position(s) within the organization responsible for compliance with all state consumer reporting laws that pertain to the consumer reports provided by the CRA for employment purposes.	CRA shall employ a minimum of one person who is responsible for CRA's development, implementation, and on-going compliance with all applicable state consumer reporting law as evidenced by written job description/s or other documentation. If multiple people are responsible, one person shall hold CRA Leadership role and overall responsibility as evidenced by written job description or other documentation.	CRA shall present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for state consumer reporting law compliance. CRA shall make this person available either in person, by phone **OR** shall provide a signed affadavit or similar document in which the person has affirmed their responsibility for state consumer reporting law compliance within the organization. If interviewed, CRA employees shall identify the person/s who can provide state consumer reporting law expertise when needed.	Compliance CRA Leader shall affirm his/her role as being responsible for state consumer reporting law compliance within the organization.
2.3 Driver Privacy Protection Act (DPPA)			
The CRA shall designate an individual(s) or position(s) within the organization responsible for compliance with the DPPA that pertain to the consumer reports provided by the CRA for employment purposes, if the CRA furnishes consumer reports that contain information subject to the DPPA.	CRA shall employ a minimum of one person who is responsible for CRA's development, implementation, and on-going compliance with all applicable DPPA law as evidenced by written job description/s or other documentation. If multiple people are responsible, one person shall hold CRA Leadership role and overall responsibility as evidenced by written job description or other documentation.	CRA shall present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for DPPA compliance. CRA shall make this person available either in person, by phone **OR** shall provide a signed affadavit or similar document in which the person has affirmed their responsibility for DPPA law compliance within the organization. If interviewed, CRA employees shall identify the person/s who can provide DPPA expertise when needed.	Compliance CRA Leader shall affirm his/her role as being responsible for DPPA compliance within the organization.
2.4 State Implemented DPPA Compliance			
If the CRA furnishes consumer reports that contain information subject to the DPPA-implementing statutes in a particular state(s), the CRA shall designate an individual(s) or position(s) within the organization responsible for compliance with state implementations of the DPPA that pertain to the products and services provided by the CRA for employment purposes.	CRA shall employ a minimum of one person who is responsible for CRA's development, implementation, and on-going compliance with all applicable state DPPA laws as evidenced by written job description/s or other documentation. If multiple people are responsible, one person shall hold CRA Leadership role and overall responsibility as evidenced by written job description or other documentation.	CRA shall present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for state DPPA law compliance. CRA shall make this person available either in person, by phone **OR** shall provide a signed affadavit or similar document in which the person has affirmed their responsibility for state DPPA law compliance within the organization. If interviewed, CRA employees shall identify the person/s who can provide state DPPA expertise when needed.	Compliance CRA Leader shall affirm his/her role as being responsible for state DPPA law compliance within the organization.
2.5 Integrity			
CRA shall not engage in bribery or any other fraudulent activity to obtain preferential treatment from a public official.	CRA shall provide written policy, procedure, or other written documentation (such as an employee handbook) clearly forbidding bribery or any other fraudulent activity to obtain preferential treatment from a public official.	CRA shall make available to auditor one or more documents which clearly forbid bribery or any other fraudulent activity to obtain preferential treatment from a public official. If interviewed, CRA employees responsible for obtaining public record information shall demonstrate knowledge of anti-bribery/fraudulent activity policy and be able to access current documentation. CRA shall affirm that they do not engage in bribery or other fraudulent activity and that CRA has never been convicted of such activity.	If CRA has been convicted of bribery or other fraudulent activity, auditor shall advise Accreditation Review Board. Board shall review specifics of case to determine whether CRA may proceed with the accreditation process.
2.6 Prescribed Notices			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall provide client all federal FCRA-required, FTC-prescribed documents which the federal FCRA mandates be provided to client by the CRA.	CRA shall provide written policy, procedure, or other written documentation describing when/how clients are provided with copies of required FTC publications.	CRA shall make available to auditor one or more documents which provide evidence that CRA has provided prescribed documents to client. CRA shall make available the person responsible for providing notices either in person, by phone **OR** shall provide a signed affadavit or similar document in which the person has affirmed his/her responsibility for compliance with notification requirements within the organization.	CRA may provide required notices as part of a Client agreement, User agreement or some other document which is signed by the client and includes client acknowledgement of receipt of required notices or provide other written documentation as to CRA's policies & procedures as to how they provide such documents. Per the FCRA, such notices currently include: 1) Notice to Users of Consumer Reports: Obligations of Users under the FCRA, and 2) A Summary of Your Rights Under the Fair Credit Reporting Act.
2.7 Agreement from Client			
Before providing consumer reports to clients, CRA shall obtain a signed agreement from client (referred to as "user" in federal FCRA) in which client agrees to meet the requirements of the federal FCRA, and applicable state and federal laws.	CRA shall provide written policy, procedure, or other written documentation describing when and how clients sign required agreement in which client agrees to comply with applicable state and federal laws, specifically including the requirements within the FCRA, and where such agreements are retained. CRA shall also provide copy of agreement document.	CRA shall present written procedure for obtaining signed agreement, copy of agreement document, and demonstrate where/how signed agreements are retained. CRA shall make available the person responsible for retaining these agreements and auditor may ask to see (but not retain a copy of) signed agreements from one or more clients. Should requested agreements predate CRA's application date for Accreditation, auditor will only look to identify language regarding compliance with FCRA. CRA employees responsible for activating client access to CRA systems/products shall demonstrate knowledge that pre-requisites exist before client is permitted access to CRA's products/systems and how the employee knows it is permissible to activiate access.	The agreement must meet requirements of FCRA, which currently include: 1) permissible purpose, 2) disclosure and authorization, 3) adverse action, 4) confidentiality, 5) compliance with all applicable laws and regulations, and 6) that client will not use consumer information in violation of any state or federal law, including equal employment opportunity laws.
Client Education			
3.1 Client Legal Responsibilities			
CRA shall have procedures in place to inform client that they have legal responsibilities when using consumer reports for employment purposes. CRA shall recommend that client consult their legal counsel regarding their specific legal responsibilities.	CRA shall provide written policy, procedure, or other documentation describing how/when clients are informed that they have legal responsibilities when using consumer reports for employment purposes and when/how CRA recommends that clients consult their legal counsel regarding client's specific legal responsibilities.	CRA shall present written procedure for informing client that they have legal responsibilities and recommending that client consult with client's legal counsel.	CRA shall inform clients that they have legal responsibilities and recommend that clients seek legal counsel as part of a Client agreement, User agreement or through some other document which is signed by the client and includes, but is not limited to, client acknowledgement of legal responsibilities. Per the FCRA, current legal responsibilities include: 1) having permissible purpose, 2) disclosing to consumer, 3) obtaining consumer authorization, 4) following prescribed adverse action procedures, 5) complying with all applicable state and federal law, and 6) obtaining, retaining, using, and destroying data in a confidential manner.

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
3.2 Client Required Documents			
CRA shall provide sample documents, or inform client of specific documents, which are needed to meet legal requirements regarding employer's procurement and use of consumer reports.	CRA shall provide written policy, procedure, or other documentation describing how/when clients are provided with sample documents, or how/when clients are informed of specific documents which are needed to meet legal requirements regarding employer's procurement and use of consumer reports. If CRA provides sample documents, such documents shall also be provided.	CRA shall present documentation describing how/when sample documents are provided and any sample documents which are provided, or how/when clients are informed of specific documents which are needed to meet legal requirements regarding employer's procurement and use of consumer reports. CRA shall make available the person responsible for providing sample documents or informing clients of the specific documents needed. If interviewed, CRA employees shall demonstrate knowledge of client-required documents, be able to access current copy of documentation, **AND/OR** CRA employees shall identify person/s to address such topics.	CRA shall provide samples of documents which are required for client to procure and use consumer reports or shall inform them of required documents. These may include, but are not limited to: 1) disclosures and authorizations to meet current federal and state requirements including special disclosure and authorization requirements in CA, OK, MN and NY; 2) required forms and/or information to obtain statewide criminal record searches in those states where currently required including AK, IN, MA, NH, NM, NV, OH, VA, WV, WY; 3) required forms and/or information to obtain driving records in those states where currently required including CA, CO, DE, GA, MD, MI, NH, OH, PA, WA. CRA may also provide sample disclosure, authorization, and/or adverse action notices. (CRA may also include other documents which must be provided to clients as described in Clause 2.6.)
3.3 Truth in Advertising			
CRA shall communicate to clients the nature of the original source, limitations, variables affecting the information available and scope of information provided by each consumer reporting product offered by the CRA.	CRA shall provide written policy, procedure, or other documentation describing how/when clients are provided with information that describes the composition of each consumer reporting product, information source/s used for each consumer reporting product, factors affecting the information, and any parameters or conditions applied by the CRA when reporting to client. CRA shall provide copy of documents used to so inform clients. If CRA provides actual consumer reports to demonstrate full and accurate consumer reporting product disclosure, all personally identified information shall be redacted.	CRA shall present written procedure for providing information to clients that accurately describes consumer reporting products, including one or more samples of provided documents. If consumer reports are used to demonstrate full and accurate consumer reporting product disclosure, all personally identified information shall be redacted and auditor will not retain copy. If interviewed, CRA employees shall demonstrate knowledge that consumer reporting product descriptions exist, where such descriptions are documented, **AND/OR** the person responsible for CRA's consumer reporting products.	Information disclosed regarding consumer reporting products shall include, but is not limited to: 1) identification of information source/s, 2) type of source, 3) scope of records searched, 4) and search methodology. It is preferred that disclosure of information source, type of source, scope of search, and search methodology be included in consumer reports. Lacking such disclosure, reports should explain how user of consumer report may obtain such information.
3.4 Adverse Action			
CRA shall inform client that there are legal requirements imposed by the federal FCRA and, in some instances, state consumer reporting laws, regarding taking adverse action against a consumer based on a consumer report. CRA shall recommend to client that they consult with counsel to develop a legally compliant adverse action policy.	CRA shall provide written policy, procedure, or other documentation describing how/when clients are informed that there are legal requirements imposed by the federal FCRA and, in some instances, state consumer reporting laws, regarding taking adverse action against a consumer based on a consumer report. CRA shall also provide copy of document used to recommend to client that they consult with counsel to develop a legally compliant adverse action policy.	CRA shall present written procedure for informing client that there are legal requirements regarding adverse action and advising client to consult with legal counsel. CRA shall make available the document/s used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients. If interviewed, CRA employees shall demonstrate knowledge of client's requirement to follow adverse action processes, be able to access current copy of documentation, **AND/OR** CRA employees shall identify person/s to address such topics.	CRA may inform client that there are legal requirements regarding adverse action as part of a Client agreement, User agreement or through some other document which is signed by the client and includes client acknowledgement. Per the FCRA, client's current legal responsibilities regarding adverse action must include: 1) providing preliminary adverse action notice to consumer, along with copy of consumer report and A Summary of Your Rights Under the Fair Credit Reporting Act, 2) allowing consumer a designated period of time to contact CRA if consumer wishes to dispute any information in consumer report, 3) providing CRA contact information, 4) providing a final adverse action notice to consumer if a final adverse employment decision is made.
3.5 Legal Counsel			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall communicate to client that they are not acting as legal counsel and cannot provide legal advice. CRA shall communicate to client the importance of working with counsel to develop an employment screening program specific to their needs. CRA shall also communicate to client the necessity to work with counsel to ensure that client's policies and procedures related to the use of CRA-provided information are in compliance with applicable state and federal laws.	CRA shall provide written policy, procedure, or other documentation describing how/when clients are informed that CRA is not acting as legal counsel and cannot provide legal advice. CRA shall provide copy of document used to so inform client and such document shall include advising client to work with legal counsel regarding client's specific screening program, policies, procedures to ensure legal compliance.	CRA shall present written procedure for informing client that CRA does not provide legal advice or act as client's legal counsel. CRA shall make available the document/s used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients. If interviewed, CRA employees shall demonstrate knowledge of CRA's position that legal counsel is not provided, be able to access current copy of documentation, **AND/OR** CRA employees shall identify person/s to address legal topics.	CRA shall inform clients that CRA does not function as legal counsel as part of a Client agreement, User agreement or through some other document which is signed by the client and includes client acknowledgement. Such acknowledgment must include, but is not limited to: 1) CRA is not legal counsel and does not provide legal advice, 2) advising client of importance of working with their legal counsel to ensure overall screening program compliance, and 3) advising clients that consumer reports provided by CRA must be used in compliance with state and federal law.
3.6 Understanding Consumer Reports			
CRA shall provide guidance to client on how to order, retrieve, read and understand the information provided in consumer reports provided by the CRA.	CRA shall provide written policy, procedure, or other documentation describing how/when clients are provided with information regarding obtaining and understanding consumer reports. CRA shall provide copy of document/s used to so inform client, shall demonstrate online tools/information (such as User Guide) provided to clients, or other method/s used to assist clients.	CRA shall present written procedure for informing client how to obtain and understand consumer reports from CRA. CRA shall make available the documents or systems used to so inform clients. If interviewed, CRA employees shall demonstrate knowledge of how such education is provided, be able to access current copy of documentation, **AND/OR** CRA employees shall identify person/s to address such topics.	CRA may provide information to clients regarding how to order, retrieve, read, and understanding consumer reports by using one or more methods which include, but are not limited to: 1) user manual/guide, 2) online training, user guides, or help system, 3) user training classes/webinars, 4) one-on-one training sessions, or 5) verbal assistance.
3.7 Information Protection			
CRA shall provide information to client regarding (1) the sensitive nature of consumer reports, (2) the need to protect such information and (3) the consumer report retention and destruction practices as outlined in the federal FCRA and the DPPA.	CRA shall provide written policy, procedure, or other documentation describing how/when clients are provided with information regarding importance of and legal requirement to protect consumer data presented in consumer reports. CRA shall provide copy of document/s used to so inform client.	CRA shall present written procedure for informing client of client's legal responsibilities regarding protection of consumer data. CRA shall make available the document/s used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients. If interviewed, CRA employees shall demonstrate knowledge of client's requirement to protect consumer data, be able to access current copy of documentation, AND/OR CRA employees shall identify person/s to address such topics.	CRA shall inform clients of client's legal requirements regarding protection of consumer data as part of a Client agreement, User agreement or through some other document which is signed by the client and includes, but is not limited to, client acknowledgement of consumer data protection responsibilities. Per the FCRA, current requirements include: 1) limiting dissemination of consumer information to only those with legitimate need, permissible purpose, and authorizated by consumer; 2) retaining consumer data in a confidential manner; and 3) destroying data in a secure manner as specified in Clause 1.10. Per the DPPA, current requirements include: protecting the privacy of consumer information which is contained in motor vehicle records, and accessing DMV records only with written consent of consumer.
Researcher and Data Standards			
4.1 Public Record Researcher Agreement			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall require a signed agreement from all non-employee public record researchers. The agreement shall clearly outline the scope of services agreed to by CRA and researcher, including jurisdictions covered, search methodology, depth of search, disclosure of findings, methodology and time frame for communication and completion of requests, methodology for confirming identity of subject of record(s), confidentiality requirements, and reinvestigation requirements.	CRA shall provide written policy, procedure, or other written documentation describing how a signed agreement covering scope of services is obtained from and retained for all current public record researchers. CRA shall also provide copy of current agreement. (Note: This agreement may also incorporate Certification requirements of Clause 4.3.)	CRA shall present written procedure for obtaining signed agreement, copy of agreement, and demonstrate where/how signed agreements are retained. CRA shall make available the person responsible for obtaining and retaining these agreements and auditor may ask to see (but not retain a copy of) signed agreements from one or more public record researchers. Agreements executed prior to the CRA's application date for Accreditation need not be in full conformance with this clause until such time the CRA undergoes the interim surveillance audit before the end of the 3rd year of the Accreditation, so as to provide the CRA time to update all researcher agreements. If interviewed, CRA employees responsible for working with public record researchers shall demonstrate understanding of requirement for signed agreement prior to utilizing services of public record researcher OR technology shall prevent utilization of public record researcher by CRA employees until CRA Leader has enabled use.	The agreement should include, but is not limited to: 1) the requirement to conduct all searches in full compliance with applicable law and regulation, 2) jurisdictions covered, 3) search methodology, 4) depth of search, 5) disclosure of findings, 6) methodology and time frame for communication and completion of requests, 7) methodology for confirming identity of subject of record(s), 8) confidentiality requirements, 9) reinvestigation requirements, and 10) the requirement for public record researcher to obtain a similar agreement from subcontractors, if subcontractors are used. In particular, the agreement should emphasize confidentiality requirements including: A) the legal requirement to treat all consumer information as confidential, B) secure data transmission, and C) secure and timely disposal of confidential information. (Note: This agreement may incorporate the Certification requirement of Clause 4.3)
4.2 Vetting Requirement			
CRA shall have procedures in place to vet or qualify new public record researchers.	CRA shall provide written policy, procedure, or other written documentation describing the requirement to and methodology used to vet or qualify new public record researchers.	CRA shall present written procedure for vetting new public record researchers, and demonstrate where/how vetting results are retained. CRA shall make available the person responsible for such vetting and auditor may ask to see (but not retain a copy of) vetting records from one or more public record researchers. If interviewed, CRA employees responsible for working with public record researchers shall demonstrate understanding of vetting requirement prior to utilizing services of public record researcher OR technology shall prevent utilization of public record researcher by CRA employees until CRA Leader has enabled use.	The vetting records may include, but are not limited to: 1) evidence of right to conduct business, such as copy of business license, articles of incorporation, state filing etc., and authentication thereof, 2) verification of required private investigator license, if such license is required, 3) completed favorable reference interviews from at least one current client, 4) verification of association memberships such as local Chamber of Commerce, Better Business Bureau, NCISS, ASIS, etc., 5) results of test searches conducted and 6) confirmation of certification under the "Criminal Record Provider Guidelines."
4.3 Public Record Researcher Certification			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall require public record researcher to certify in writing that they will conduct research in compliance with all applicable local, state and federal laws, as well as in the manner prescribed by the jurisdiction which maintains the official record of the court; never obtain information through illegal or unethical means; and utilize document disposal and/or destruction methods pursuant to the federal FCRA.	CRA shall provide written policy, procedure, or other written documentation describing how/when/where the signed certification is obtained from and retained for all current public record researchers. CRA shall also provide copy of current certification. (Note: This certification may be incorporated in or an appendix to the "Public Record Researcher Agreement" described in Clause 4.1.)	CRA shall present written procedure for obtaining signed certification, copy of certification, and demonstrate where/how signed certifications are retained. CRA shall make available the person responsible for retaining these certifications and auditor may ask to see (but not retain a copy of) signed certifications from one or more public record researchers. (Note: This certification may be part of the "Public Record Researcher Agreement" described in Clause 4.1.) Certifications executed prior to the CRA's application date for Accreditation need not be in full conformance with this clause until such time the CRA undergoes the interim surveillance audit before the end of the 3rd year of the Accreditation, so as to provide the CRA time to update all researcher certifications. If interviewed, CRA employees responsible for working with public record researchers shall demonstrate understanding of certification requirement prior to utilizing services of public record researcher OR technology shall prevent utilization of public record researcher by CRA employees until CRA CRA Leader has enabled use	The Certification in which the Public Record Researcher agrees must include, but is not limited to, the following: 1) to comply with all applicable local, state and federal laws, as well as in the manner prescribed by the jurisdiction which maintains the official record of the court; 2) to obtain information only through legal and ethical means; and 3) to dispose of or destroy confidential documents in a secure manner per FTC document destruction rule. (Note: This certification may be part of the "Public Record Researcher Agreement" described in Clause 4.1.)
4.4 Errors and Omissions Coverage (E&O)			
CRA shall obtain proof of public record researcher's Errors and Omissions Insurance. If public record researcher is unable to provide proof of insurance, CRA shall maintain coverage for uninsured and/or underinsured public record researcher.	CRA shall provide written policy, procedure, or other written documentation describing the requirement to and method used to verify public record researcher's Errors and Omissions insurance and that such insurance remains in force. If researcher does not have or cannot prove existing coverage, CRA shall provide copy of CRA's insurance policy which contains E&O coverage for uninsured/underinsured public record researchers.	CRA shall present written procedure for obtaining proof of public record researcher's E&O insurance and demonstrate where/how such proof documentation is retained. CRA shall make available the person responsible for retaining this proof and auditor may ask to see (but not retain a copy of) such proof from one or more public record researchers. In addition, auditor may ask to see (but not retain copy of) CRA's E&O insurance policy in which coverage for uninsured/underinsured public record researchers is provided. If interviewed, CRA employees responsible for working with public record researchers shall demonstrate understanding of E&O requirement prior to utilizing services of public record researcher OR technology shall prevent utilization of public record researcher by CRA employees until CRA CRA Leader has enabled use	The E&O insurance should be in force and cover CRA and CRA public record researchers. No specific amount is required but a minimum of two million in coverage is recommended.
4.5 Information Security			
CRA shall provide a secure means by which public record researchers will receive orders and return search results.	CRA shall provide written policy, procedure, or other written documentation describing the requirement to and method used to secure and protect consumer information when such information is being transmitted to and returned by public record researchers.	CRA shall present written procedure for sending consumer information to and receiving consumer information from public record researchers. CRA shall make available the person responsible for security of transmitted consumer information and auditor may ask to see demonstration of security tools in use. For each transmission method, CRA may be asked to demonstrate the security controls which are in use.	Security procedures for personally identifiable information should include, but are not limited to: 1) all transmissions should directed to a named party, 2) all transmissions must be clearly marked as "CONFIDENTIAL" and include a request to notify sender if received by someone other than named party, 3) if faxed, a cover page should always be used and must not contain any personally identifiable information, 4) if faxed, CRA shall have verified receiving fax is in a non-public location, 5) if transmitted using CRA network, such network should be secured using a minimum of 128 SSL, 6) if transmitted via Internet, data shall be encrypted or protected in a comparable manner

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
4.6 Auditing Procedures			
CRA shall maintain auditing procedures for quality assurance in regard to their active public record researchers.	CRA shall provide written policy, procedure, or other written documentation describing the requirement to and method used to audit public record researchers in order to actively monitor quality of researcher work.	CRA shall present written documentation for auditing public record researchers. CRA shall make available the person responsible for such audits and auditor may ask to see (but not retain copy of) audit results for one or more public record researchers.	Audit procedures for public record researchers may include, but are not limited to: 1) an established protocol for auditing researchers, 2) sending research requests where result is already known, 3) how returned results are compared to expected results, and 4) process for dealing with researcher errors up to and including termination of services. It is recommended that test cases be entered in a log with results that may include,: A) date of test, B) unique identifier such as order number or subject name plus last four digits of SSN, C) results returned, D) whether results were as expected, and E) any remedial actions taken
4.7 Identification Confirmation			
CRA shall follow reasonable procedures to assure maximum possible accuracy when determining the identity of a consumer who is the subject of a record prior to reporting the information. CRA shall have procedures in place to notify client of any adverse information that is reported based on a name match only.	CRA shall provide written policy, procedure, or other written documentation describing procedures used to assure maximum possible accuracy when determining the identity of a consumer who is the subject of a record prior to reporting the information. CRA shall provide written policy, procedure, or other written documentation describing procedures used to notify client of any adverse information that is reported based on a name match only.	CRA shall present written documentation for assuring maximum possible accuracy when determining the identity of a consumer who is the subject of a record prior to reporting the information. CRA shall present written documentation for notifying client of any adverse information that is reported based on a name-match only. CRA shall make available the person responsible for ensuring compliance with CRA's policy in regard to assuring maximum possible accuracy when reporting adverse information based on a name-match only. CRA employees responsible for such identification shall demonstrate knowledge of identification requirement and be able to access current documentation	Recommended procedures may include, but are not limited to: 1) matching a minimum of two identifiers which may include name, date of birth, SSN, current and previous addresses, and/or driver's license number; and/or 2) stating in client report which identifiers were used to conclude a match existed, and/or 3) stating information is based on a name match only, if CRA reports based on single identifier.
4.8 Jurisdictional Knowledge			
The CRA shall designate a qualified individual(s) or position(s) within the organization responsible for understanding court terminology, as well as understanding the various jurisdictional court differences if CRA reports court records.	CRA shall employ or retain a minimum of one person who is responsible for CRA's understanding, implementation, and on-going use of court terminology as well as variances which may exist at the jurisdictional level as evidenced by job description or other documentation. If multiple people are responsible, one person shall hold CRA Leadership role and overall responsibility as evidenced by written job description or other documentation.	CRA shall present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for court/jurisdictional knowledge. CRA shall make this person available either in person, by phone OR shall provide a signed affidavit or similar document in which the person has affirmed their responsibility for court/jurisdictional knowledge within the organization and that s/he is qualified to hold such responsibility. If interviewed, this individual shall demonstrate knowledge of court and jurisdictional knowledge as well as identifying resources for additional information. If interviewed, CRA employees shall identify the person(s) who can provide court/jurisdictional expertise when needed.	An individual may be qualified if they have one or more of the following: 1) criminal justice degree, 2) law enforcement experience, 3) legal experience, 4) court experience, 5) investigator experience, and/or 6) three years work experience with court records with the current CRA employer or other CRA's. Compliance CRA Leader shall affirm his/her role as being responsible for court/jurisdictional knowledge within the organization and that s/he is qualified to hold such responsibility.
	CRA shall provide qualifications of Court/Jurisdictional Knowledge CRA Leader.	CRA shall provide evidence of qualifications by presenting resume, educational credentials, experience, and/or other documentation.	N/A
Verification Service Standards		**DEFINITION**: As used in this section, "Verification" refers to academic, employment, reference, and other checks conducted using information which is not public. "Outsourced Verification Services" (Clause 5.8) refers to a business arrangement in which the CRA contracts with another company and that company conducts employment, academic, and/or reference checks on behalf of the CRA and return results to the CRA. Outsourcing criminal record checks to public record field researchers **ARE NOT** considered "Outsourced Verification Services."	
5.1 Verification Accuracy			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall maintain reasonable procedures to assure maximum possible accuracy when obtaining, recording and reporting verification information.	CRA shall provide written policy, procedure, or other documentation used to reasonably ensure accuracy and thoroughness in the verification process.	CRA shall make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure verification accuracy. If interviewed, CRA employees responsible for verification accuracy shall demonstrate knowledge of accuracy requirement, describe methodology by which they learn how to obtain accurate verifications. CRA employees responsible for verification accuracy shall be able to access current copy of documentation, AND/OR CRA employees shall identify person/s responsible for accuracy.	CRA may provide information regarding verification accuracy to employees who are responsible for such accuracy by using various methods which may include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual may be used. Methods used to reasonably ensure verification accuracy may include, but are not limited to: confirmation of identity through verification of SSN, full name, and/or date of birth; 2) confirmation of information source name, address, and contact information; and 3) soliciting information from a source rather than providing leading information; i.e., asking for job title rather than providing title and asking for confirmation.
5.2 Current Employment			
CRA shall have procedures in place to contact consumer's current employer directly only when authorized by client and/or consumer.	CRA shall provide written policy, procedure, or other documentation used to ensure consumer's current employer is not contacted direclty unless consumer and/or client has provided explicit authorization.	CRA shall make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure current employer is not directly contacted without explicit authorization by the consumer and/or client. If interviewed, CRA employees responsible for verification of current employment shall demonstrate knowledge of authorization requirement and describe methodology by which they learn about such requirement. CRA employees responsible for current employer contact shall be able to access current copy of documentation, AND/OR CRA employees shall identify person/s responsible for such contact.	CRA may provide information regarding verification of current employment to employees who are responsible for such verification by using various methods which may include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual should be used. Methods used to reasonably ensure consumer's current employer is directly contacted only with authorization may include, but are not limited to: 1) authorization provided on employment application, 2) explicit authorization provided within Disclosure/Authorization signed by consumer, 3) Specific directive provided by client, AND/OR 4) technology shall prevent verification of current employment by CRA employees until CRA Leader has so enabled.
5.3 Diploma Mills			
When attempting educational verifications from known or suspected diploma mills, CRA shall have procedures in place to advise client of such.	CRA shall provide written policy, procedure, or other documentation used to reasonably ensure validity of academic institution and advise client of findings when the institution is a known or suspected "diploma mill."	CRA shall make available to auditor tools or systems used to reasonably ensure identification of diploma mills and to advise client when applicable. If interviewed, CRA employees responsible for verification of academic credentials received from diplomas mills and advising client shall demonstrate knowledge of diploma mills and describe methodology by which they learn about such diplomas mills and how to advise clients. CRA employees responsible for verification of academic credentials and advising clients shall be able to access current copy of documentation, AND/OR CRA employees shall identify person/s responsible for such activity.	CRA may provide information regarding verification of academic credentials from diploma mills to employees who are responsible for such verification by using various methods which include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual should be used. Methods used to reasonably ensure identification of diploma mill include, but are not limited to: 1) a check of CRA's existing database or list of known diploma mills, 2) a check with the council for higher education, 3) state education departments, and/or 4) an internet search of the academic institution. When advising client regarding diploma mills and putting such information in consumer report, CRA shall avoid "absolutes" and rather use language similar to "academic institution appears to be a diploma mill because it sells academic credentials..."
5.4 Procedural Disclosures			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall provide full disclosure to clients about general business practices regarding number of attempts to verify information, what constitutes an "attempt," locate fees, fees charged by the employer or service provider and standard question formats prior to providing such services.	CRA shall present written policy, procedure, client education material or other written documentation methodology used to provide full disclosure to a client about general business practices regarding number of attempts to verify information, what constitutes an "attempt," locate fees, fees charged by the employer or service provider and standard question formats prior to providing such services.	CRA shall make available to auditor tools or systems used to disclose to client general practices regarding verification practices including attempts to verify, fees, question formats, etc. CRA shall present written procedure for providing information to clients that accurately describes products, including one or more samples of provided documents. If consumer reports are used to demonstrate full and accurate procedural disclosure, all personally identified information shall be redacted and auditor will not retain copy. If interviewed, CRA employees shall demonstrate knowledge that procedural requirements exist, where such requirements are documented, AND/OR the person responsible for CRA's products	CRA shall provide information to employers regarding general verification business practices by using various methods which include, but are not limited to: 1) product descriptions, 2) statement of work documents, 3) written agreements, and/or detail provided in the verification itself. Disclosed information regarding general verification business practices includes, but is not limited to: 1) number of attempts to verify information, 2) what constitutes an "attempt," 3) fees charged by the employer or service provider, and 4) standard question formats.
5.5 Verification Databases			
If CRA compiles, maintains and resells employment or educational verification information, CRA shall have procedures in place to ensure that data compiled and stored is accurate, including procedures for handling consumer disputes.	CRA shall present written policy, procedure or other written documentation used to ensure that data compiled and stored is accurate, including procedures for handling consumer disputes. If CRA does not compile, maintain, and resell employment or education information, CRA shall provide written affirmation to that effect.	CRA shall make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure data compiled and stored is accurate. If interviewed, CRA employees responsible for accuracy of stored data shall demonstrate knowledge of accuracy requirement and describe methodology used to ensure accuracy. CRA employees responsible for accuracy of stored data shall be able to access current copy of documentation, identify person/s responsible for accuracy of stored data, **AND/OR** utilize technology to control the addition or deletion of information in the database/s.	This clause addresses organizations that compile information for potential future use or sale. CRA may provide information regarding accuracy of stored data to employees who are responsible for such accuracy by using various methods which include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual may be used. Methods used to reasonably ensure accuracy of stored data include, but are not limited to: criteria for inclusion into the database, criteria for redaction from the database, criteria for correcting inaccuracies and handling consumer disputes.
5.6 Use of Stored Data			
If CRA provides investigative consumer reports from stored data, CRA shall have procedures in place to ensure the CRA does not provide previously reported adverse information unless it has been re-verified within the past three months, or for a shorter time if required by state or local law.	CRA shall present written policy, procedure or other written documentation to ensure CRA does not provide previously reported adverse information stored in CRA's database unless it has been re-verified within the past three months, or for a shorter time if required by state or local law. If CRA does not utilize stored data, CRA shall provide written affirmation to that effect.	CRA shall make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure that adverse data older than 3 months (or less if so required by applicable law) in CRA's database is re-verified prior to such information being included in a new consumer report. If interviewed, CRA employees responsible for use of such data shall demonstrate knowledge of 3-month re-verification requirement and describe methodology used to ensure compliance. CRA employees responsible for use of stored data shall be able to access current copy of documentation, shall identify person/s responsible for use of stored data, **AND/OR** technology shall prevent utilization of stored adverse data which is older than 90 days.	CRA may provide information regarding use of stored adverse data to employees who are responsible for using such data by using various methods which include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or 5) availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual may be used. Such information and/or training shall include what constitutes "adverse" information for different types of background checks through: 1) definition, 2) examples, and/or 3) by referring CRA employees to designated expert.
5.7 Documentation of Verification Attempts			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall have procedures in place to document all verification attempts made and the result of each attempt, in completing all verification services.	CRA shall present written policy, procedure, or other written documentation used to ensure that all attempts made to verify information are fully documented.	CRA shall make available to auditor tools, systems, or methods used to capture attempts to verify and related information. If a manual process, CRA shall present written procedure for capturing such information. If consumer reports are used to demonstrate captured attempts and related information, all personally identified information shall be redacted and auditor will not retain copy. If interviewed, CRA employees shall demonstrate knowledge that attempts to verify must be documented, where such requirements are documented, identify the person responsible for CRA's products and processes, **AND/OR** technology shall automatically capture attempts to verify and related information.	CRA may provide information regarding attempts to verify and related information to employees who are responsible for data verification by using various methods which include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual may be used. Information regarding attempts to verify should include, but is not limited to: 1) date and time of contact or attempted contact, 2) method of contact (such as phone number dialed, fax number used, email address used, address to which information was mailed, etc.), 3) name and title of contact, 4) results of attempt, and 4) the CRA employee who made the attempt or obtained information
5.8 Outsourced Verification Services			
CRA shall require a signed agreement from all providers of outsourced verification services. The agreement shall clearly outline the scope of services to be provided, verification methodology, documentation of verification efforts, disclosure of findings, time frame for communication and completion of requests, confidentiality requirements, reinvestigation requirements and other obligations as furnishers of information under the federal FCRA.	CRA shall provide written policy, procedure, or other written documentation describing how a signed agreement covering scope of services is obtained from and retained for all current outsourced verification service providers. CRA shall also provide copy of current agreement. If CRA does not utilize stored data, CRA shall provide written affirmation to that effect.	CRA shall present written procedure for obtaining signed agreement, copy of agreement, and demonstrate where/how signed agreements are retained. CRA shall make available the person responsible for obtaining and retaining these agreements and auditor may ask to see (but not retain a copy of) signed agreements from one or more outsourced verification service providers. If interviewed, CRA employees responsible for working with these providers shall demonstrate understanding of requirement for signed agreement prior to utilizing services of provider OR technology shall prevent utilization of provider by CRA employees until CRA CRA Leader has enabled use.	The agreement should include, but is not limited to: 1) the requirement to conduct all verifications in full compliance with applicable law and regulation, 2) scope of services provided, 3) methods used to obtain information, 4) time frame for communication and completion of requests, 5) methodology for confirming identity of subject of verification, 6) confidentiality requirements, 7) reinvestigation requirements, 8) documented "attempts to verify" per Clause 5.4, 9) background check requirements and acceptable results for provider's employees, and 10) signed non-disclosure agreements from provider's employees. In particular, the agreement should emphasize confidentiality requirements including: A) the legal requirement to treat all consumer information as confidential, B) secure data transmission, and C) secure and timely disposal of confidential information.
5.9 Conflicting Data			
Should CRA receive information from the verification source subsequent to the delivery of the consumer report, and as a direct result of the initial inquiry, that conflicts with originally reported information, and that new information is received within 120 days of the initial report, (or as may be required by law), CRA shall have procedures in place to notify client of such information.	CRA shall provide written policy, procedure, or other documentation describing how conflicting data, when received within 120 of report completion and as a direct result of original inquiry, is provided to client who originally ordered such report.	CRA employees responsible for reporting conflicting data as described in 5.9 shall demonstrate knowledge of proper procedures and be able to access current copy of documentation.	CRA may provide information regarding processing and reporting of conflicting data to employees who have this responsibility by using various methods which include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual may be used. Information regarding handling and reporting of conflicting data should include, but is not limited to: 1) confirmation that conflicting information is specifically related to same consumer, same customer, and original report, 2) verification of the authenticity of the conflicting information and its source, 3) method used to update report, and 4) method used to provide updated information to consumer and customer, and 5) the form in which the update is provided.
5.10 Professional Conduct			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall train all employees engaged in verification work on procedures for completing verifications in a professional manner.	CRA shall provide written policy, procedure, or other documentation which instructs all CRA employees engaged in verification work on procedures for completing verifications in a professional manner.	CRA shall make available to auditor any materials used to train CRA employees engaged in verification work on professionalism when conducting verifications. If interviewed, CRA employees who conduct such verification work shall describe training which was received.	CRA may provide information to employees regarding professionalism when conducting verifications by using one or more methods which include, but are not limited to: 1) written material, 2) online training, 3) training classes/webinars, 4) one-on-one training sessions, and/or 5) on-the-job training.
5.11 Authorized Recipient			
If CRA is requesting verification by phone, fax, email or mail, CRA shall have procedures in place to confirm that verification request is directed to an authorized recipient.	CRA shall provide written policy, procedure, or other documentation used to require that verification requests are directed to authorized recipients.	CRA shall present written procedure for confirming a verification request is being sent to authorized individual. If interviewed, CRA employees responsible for processing verification requests shall demonstrate knowledge of proper authentication procedures and shall be able to access current copy of documentation.	Procedures used to ensure verification requests are sent to an authorized recipient may include, but are not limited to: 1) confirming method used by information source to provide verification information, 2) confirming company/institution name and address matches that provided by consumer, and 3) obtaining name and title of person to whom request will be sent.
Miscellaneous Business Practices			
6.1 Character			
Owners, officers, principals and employees charged with the enforcement of company policy must consent to undergo a criminal records check and be found free of convictions for any crimes involving dishonesty, fraud or moral turpitude.	CRA shall provide written policy, procedure, or other written documentation describing the requirement for and method used to conduct criminal history record checks on owners, principals, and employees charged with enforcement of company policy to confirm these individuals are free of convictions for any crimes involving dishonesty, fraud, or moral turpitude. CRA shall affirm in writing that owners, officers, principals and employees charged with the enforcement of company policy are free of convictions for any crimes involving dishonesty, fraud or moral turpitude.	CRA shall present written procedure for conducting criminal history record checks on owners, principals and employees charged with the enforcement of company policy. CRA shall also demonstrate how results are reviewed for acceptability and where records are retained. CRA shall make available the person responsible for these checks and auditor may ask to see (but not retain a copy of) criminal history check results.	This clause refers only to the entity being accreditated and not any parent company. It covers owners, managers, and supervisory personnel who are charged with enforcement of company policy. See Clause 6.10 for all CRA employees. Criminal record checks shall be free of criminal convictions for dishonesty, fraud or moral turpitude.
6.2 Insurance			
CRA shall maintain errors and omissions insurance. If CRA does not maintain errors and omission insurance, CRA must self-insure in a manner compliant with its state's insurance requirements.	CRA shall provide copy of Certificate of Insurance listing errors and omissions policy coverage amount. If CRA does not maintain errors and omissions insurance, CRA must provide documentation that they have self insured in conformance with state requirements.	None	None
6.3 Client Authentication			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall have a procedure to identify and authenticate all clients prior to disclosing consumer reports or other consumer information. The procedure shall require the CRA to maintain written records regarding the qualification of each client who receives consumer reports or other consumer information.	CRA shall provide written policy, procedure, or other written documentation describing the requirement for and method used to authenticate clients prior to providing consumer reports or any consumer information to client.	CRA shall present written procedure for athenticating new clients, and demonstrate where/how authentication results are retained. CRA shall make available the person responsible for such authentication and auditor may ask to see (but not retain a copy of) authentication records from one or more client companies. If interviewed, CRA employees responsible for providing consumer information to clients shall demonstrate understanding of authentication requirement prior to providing consumer information to clients OR technology shall prevent providing such information to clients until CRA Leader has enabled process	Client authentication methods may include, but are not limited to: 1) obtaining evidence of right to conduct business, such as copy of business license, articles of incorporation, state filing etc., and authentication thereof, 2) verification of working business phone, fax, email, and website, 3) verification of listing in business directories such as yellow pages, Hoover's, Dun and Bradstreet, etc., and 4) onsite inspection to confirm business facility exterior and interior appearance meet common business norms for this type of business.
6.4 Vendor Authentication			
CRA shall have a procedure to identify and authenticate all vendors prior to disclosing consumer information. The procedure shall require the CRA to maintain written records regarding the qualification of each vendor who receives consumer information.	CRA shall provide written policy, procedure, or other written documentation describing the requirement for and method used to authenticate vendors prior to disclosing any consumer information to vendor.	CRA shall present written procedure for athenticating new vendors, and demonstrate where/how authentication results are retained. CRA shall make available the person responsible for such authentication and, if interviewed, this person shall demonstrate understanding of authentication requirements. Auditor may ask to see (but not retain a copy of) authentication records from one or more vendor companies.	In the case of vendors which are recognized and commonly utilized by CRAs, a signed agreement between the vendor and CRA will suffice as authentication. Such vendors include but are not limited to: major credit bureaus, repositories of education and employment data, motor vehicle record resellers, etc. For unknown vendors, authentication records may include, but are not limited to: 1) onsite inspection results, 2) evidence of right to conduct business, such as copy of business license, articles of incorporation, state filing etc., and authentication thereof, 3) verification of working phone/fax numbers, website, email, 4) reference through a minimum of one independent third-party, and/or 5) previous experience of CRA when working with vendor.
6.5 Consumer Authentication			
CRA shall develop and implement requirements for what information consumers shall provide as proof of identity prior to providing file disclosure to the consumer. The CRA shall maintain procedures to document the information used to identify each consumer to whom file disclosure is provided.	CRA shall provide written policy, procedure, or other written documentation describing how/when consumer authentication/identification occurs prior to disclosing consumer information and where record of such authentication is kept.	CRA shall present written procedure for confirming consumer's identify prior to providing any consumer information to such person. Auditor may ask to see demonstration of consumer identifcation, how CRA representative confirms identify of consumer, and where record of authenthication is retained.	Consumer identification processes may include, but are not limited to confirmation of: 1) full name, 2) date of birth, 3) street address used on application or authorization document, 4) last four digits of SSN, and 5) driver's license number.
6.6 Document Management			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall have a written record retention and destruction policy pursuant to the federal FCRA.	CRA shall provide written policy, procedure, or other written documentation describing CRA's record retention and destruction practices.	CRA shall present written document retention and destruction policy. CRA shall make available the person responsible for document retention and destruction. If interviewed, this person shall demonstrate understanding of retention and destruction requirements.	CRA's should retain records to comply with the limitation of liability action per the FCRA, which is currently "...not later than the earlier of (1) 2 years after the date of discovery by the plaintiff of the violation that is the basis for such liability; or (2) 5 years after the date on which the violation that is the basis for such liability occurs." CRA's are subject to the FTC's document destruction rule which currently requires secure destruction through means that are reasonable and appropriate to prevent the unauthorized access to or use of information in a consumer report. For example, establishing and complying with policies to: burn, pulverize, or shred papers so that the information cannot be read or reconstructed; destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed; or conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule.
6.7 Employee Certification			
CRA shall require all workers to certify they will adhere to the confidentiality, security and legal compliance practices of the CRA.	CRA shall provide written policy, procedure, or other written documentation describing how/when CRA obtains from all employees a certification in which employee agrees to adhere to the CRA's confidentiality, security, and legal compliance practices and where such certifications are retained.	CRA shall present written procedure for obtaining employee written certification that employee will adhere to CRA's confidentiality, security, and legal compliance practices. If questioned, CRA employees shall confirm they were required to provide this certification. Auditor may ask to see, but not retain copy of, the certification signed by one or more employees.	Certification language may include, but is not limited to, agreement by employee to: 1) hold, use, and destroy all client and consumer information in a secure manner, 2) provide consumer information to third parties only after following defined authentication procedures, 3) abide by physical security practices, 4) abide by information security practices, and 5) follow all compliance practices of the CRA.
6.8 Worker Training			
CRA shall provide training to all workers on confidentiality, security and legal compliance practices of the CRA.	CRA shall provide written policy, procedure, or other documentation which describes the requirement for and methodology used to train CRA employees on the confidentialiy, security, and legal compliance procedures of the CRA.	CRA shall present written procedure for providing training to employees regarding confidentiality, security and legal compliance practices of CRA. CRA shall make available to auditor any materials used for such training. If interviewed, CRA employees shall describe training which was received.	CRA may provide training to employees regarding confidentiality, security, and legal compliance practices by using one or more methods which include, but are not limited to: 1) written material, 2) online training, 3) training classes/webinars, 4) one-on-one training sessions, and/or 5) on-the-job training.
6.9 Visitor Security			
CRA shall utilize a visitor security program to ensure visitors do not have access to consumer information.	CRA shall provide written policy, procedure, or other documentation which describes the visitor security program and how visitors are prevented from accessing consumer information.	CRA shall present written procedure for ensuring visitor security which prevents access to consumer information. CRA shall make available theperson responsible for visitor security program. This person shall be able to describe and/or provide documentation related to visitor security and access control. If questioned, CRA employees shall demonstrate knowledge of visitor security policy.	Visitor security policy must include method/s wihch prevent visitors from accessing consumer information. These methods may include, but are not limited to: 1) use of sign in/out registry, 2) issuance of temporary badges, 3) situations in which a CRA employee must escort the visitor, 4) controlled access to systems and data, and 5) controlled access to areas of facility in which consumer information is readily available on screens or hard copy.
6.10 Employee Criminal History			

Clause	Measure & Documentation Typically Subject to Desk Audit	Potential Verification for Onsite Audit	Attributes of and Suggestions for Onsite Audit What auditor should look for in policy, procedure, activity
CRA shall conduct a criminal records check on all employees with access to consumer information when such searches can be conducted without violating state or federal law. These searches shall be conducted at least once every two years for the duration of their employment. Criminal offenses shall be evaluated to determine initial or continued employment based upon their access to consumer information and state and federal laws.	CRA shall provide written policy, procedure, or other documentation which describes the requirement for and methodology used to conduct criminal record checks every two years on all employees with access to consumer information when such criminal record searches may be conducted without violating state or federal law. The documentation shall describe how results of these checks are evaluated in relation to employee's access to consumer information, state/federal law, and initial or continued employment.	CRA shall present written procedure for conducting a criminal records check every two years on all employees with access to consumer information. CRA shall make available the person responsible for retaining these reports and auditor may ask CRA to demonstrate where/how reports are retained as well as to see (but not retain a copy of) completed criminal records check report from one or more employees.	The evaluation of employee criminal check results and employment/continued employment must comply with applicable state or federal law in relation to work performed by the CRA and licenses held by the CRA (such as private investigator). The evaluation of employee criminal check results may also include, but are not limited to: 1) position employee holds or will hold with CRA, 2) the nature of the offense/s, 3) the time elapsed since the offense/s occurred, 4) the conduct of the employee since the offense/s, 5) evidence of rehabilitation, and 6) employment history.
6.11 Quality Assurance			
CRA shall have procedures in place to reasonably ensure the accuracy and quality of all work product.	CRA shall provide written policy, procedure, or other documentation describing the methods used to reasonably ensure the accuracy and quality of all work product.	CRA shall present procedures which are in place to reasonably ensure the accuracy and quality of all work product. CRA shall make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure accuracy and quality in all work product. If interviewed, CRA employees responsible for work product shall demonstrate knowledge of accuracy and quality requirements, describe methods used to ensure quality and accuracy, shall be able to access current copy of documentation, and shall identify person/s responsible for providing on-the-job quality and accuracy leadership.	CRA may provide information regarding quality and accuracy of work product to employees who are responsible for such quality and accuracy by using various methods which include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual may be used.
6.12 Responsible Party			
CRA shall have on staff one person designated to oversee and administer the accreditation processes and future compliance by the CRA, including enforcement of the standard by all concerned. This person shall be vested with the responsibilities and authority attendant to this task, and shall be the CRA contact for the auditor and accreditation related matters for NAPBS®.	CRA shall employ a minimum of one person who is responsible for CRA's accreditation activity and on-going compliance with applicable standards/requirements as evidenced by written job description/s or other documentation. If multiple people are responsible, one person shall hold overall responsibility as evidenced by written job description or other documentation.	CRA shall present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for accreditation activity and on-going compliance. CRA shall make this person available either in person, by phone **OR** shall provide a signed affadavit or similar document in which the person has affirmed their responsibility for accreditation activity and on-going compliance within the organization and that s/he is qualified to hold such responsibility. If interviewed, CRA employees shall identify the person/s who can provide accreditation expertise when needed.	The person responsible for overall accreditation shall affirm his/her role as being responsible for accreditation/certification activity and on-going compliance within the organization and that s/he is qualified to hold such responsibility.
Miscellaneous Notes: Concepts of "Opportunity for Improvement" (OFI) and "Controlled Document"			