

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
<b>Data Information and Security</b>			
DEFINITION: Consumer information includes any information identifiable to one or more consumers, including that found in vendor reports,			
<b>1.1 Information Security</b> CRA shall have a written information security policy. CRA shall designate one or more qualified 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.
	CRA shall demonstrate that individual who is responsible for information security program is qualified to hold such responsibility.	CRA shall provide evidence of qualifications by presenting resume, educational credentials, experience, and/or other documentation.	N/A
<b>1.2 Data Security</b>			
CRA shall have procedures in place to reasonably protect consumer information 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 possession, 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.
<b>1.3 Intrusion and Data Security</b>			
CRA shall have procedures in place to reasonably 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) debrief to prevent future occurrences
<b>1.4 Stored Data Security</b>			
CRA shall have procedures in place to reasonably 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.
<b>1.5 Password Protocol</b>			
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.
<b>1.6 Electronic Access Control</b>			
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 effectively administer access rights. Users shall only be given the access reasonably 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.
<b>1.7 Physical Security</b>			
CRA shall have procedures in place to control physical access to all areas that contain consumer information.	CRA shall provide written policy, procedure or other documentation explaining how access to areas 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.
<b>1.8 Consumer Information Privacy Policy</b>			

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.
<b>1.9 Unauthorized Browsing</b>			
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
<b>1.10 Record Destruction</b>			
When records are to be destroyed or disposed of, CRA shall follow FTC guidelines and take measures to reasonably 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.
<b>1.11 Consumer Disputes</b>			
CRA shall have procedures in place for handling and documenting a consumer dispute as required by 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.)
<b>1.12 Sensitive Data Masking</b>			

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 and industry practice.	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.	CRA employees shall demonstrate knowledge of proper procedures for use of SSN's and other sensitive data elements 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 <b>AND if applicable</b> , the use of technology to protect SSN's and other sensitive data elements.	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 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 sensitive data elements outside the CRA environment, secure transport methods shall be used.
<b>1.13 Database Criminal Records</b>			
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) utilize contemporaneous notice	CRA shall provide written policy, procedure, or other documentation describing method/s used to comply with current FCRA requirements of source verification or contemporaneous notice.	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.
<b>Legal and Compliance</b>			
<b>2.1 Designated Compliance Person(s)</b>			
The CRA shall designate a qualified individual(s) or position(s) within the organization responsible for demonstrating a thorough understanding of and compliance with all sections of the federal FCRA that pertain to the products and services provided by the CRA.	CRA shall employ or retain 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 <b>OR</b> shall provide a signed affidavit or similar document in which the person has affirmed their responsibility for FCRA 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 FCRA expertise when needed.	CRA Compliance Leader shall affirm his/her role as being responsible for FCRA compliance within the organization and that s/he is qualified to hold such responsibility.
	CRA shall provide qualifications of CRA's FCRA Compliance Leader.	CRA shall provide evidence of qualifications by presenting resume, educational credentials, experience, and/or other documentation.	N/A
<b>2.2 State Consumer Reporting Laws</b>			
The CRA shall designate a qualified individual(s) or position(s) within the organization responsible for demonstrating a thorough understanding of and compliance with state consumer reporting laws that pertain to the products and services provided by the CRA.	CRA shall employ or retain 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 <b>OR</b> shall provide a signed affidavit or similar document in which the person has affirmed their responsibility for state consumer reporting law 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 state consumer reporting law expertise when needed.	CRA Compliance Leader shall affirm his/her role as being responsible for state consumer reporting law compliance within the organization and that s/he is qualified to hold such responsibility.

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 qualifications of State Consumer Reporting Law Compliance CRA Leader.	CRA shall provide evidence of qualifications by presenting resume, educational credentials, experience, and/or other documentation.	N/A
<b>2.3 Driver Privacy Protection Act (DPPA)</b>			
The CRA shall designate a qualified individual(s) or position(s) within the organization responsible for demonstrating a thorough understanding of and compliance with the DPPA that pertain to the products and services provided by the CRA.	CRA shall employ or retain 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 <b>OR</b> shall provide a signed affidavit or similar document in which the person has affirmed their responsibility for DPPA law 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 DPPA expertise when needed.	CRA Compliance Leader shall affirm his/her role as being responsible for DPPA compliance within the organization and that s/he is qualified to hold such responsibility.
	CRA shall provide qualifications of DPPA Compliance CRA Leader.	CRA shall provide evidence of qualifications by presenting resume, educational credentials, experience and/or other documentation.	N/A
<b>2.4 State Implemented DPPA Compliance</b>			
The CRA shall designate a qualified individual(s) or position(s) within the organization responsible for demonstrating a thorough understanding of and compliance with state implementations of the DPPA that pertain to the products and services provided by the CRA.	CRA shall employ or retain 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 <b>OR</b> shall provide a signed affidavit or similar document in which the person has affirmed their responsibility for state DPPA law 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 state DPPA expertise when needed.	CRA Compliance Leader shall affirm his/her role as being responsible for state DPPA law compliance within the organization and that s/he is qualified to hold such responsibility.
	CRA shall provide qualifications of State DPPA Compliance CRA Leader.	CRA shall provide evidence of qualifications by presenting resume, educational credentials, experience, and/or other documentation.	N/A
<b>2.5 Integrity</b>			
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 any principal of a 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.
<b>2.6 Prescribed Notices</b>			

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 customers and consumers 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 <b>OR</b> shall provide a signed affidavit or similar document in which the person has affirmed his/her responsibility for compliance with notification requirements within the organization and that s/he is qualified to hold such responsibility.	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. Per the FCRA, such notices currently include: 1) Notice to Users of Consumer Reports: Obligations of Users under the FCRA, 2) A Summary of Your Rights Under the Fair Credit Reporting Act, and 3) Remediating the Effects of Identity Theft.
<b>2.7 Agreement from Client</b> 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, including permissible purpose, disclosure and authorization, state or federal EEOC compliance and adverse action.	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. 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 activate access.	The agreement must meet requirements of FCRA, which currently include: 1) permissible purpose, 2) disclosure and authorization, 3) adverse action procedures, 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.
<b>Client Education</b>			
<b>3.1 Client Legal Responsibilities</b>			
CRA shall have procedures in place to inform client of client's legal responsibilities when using consumer reports for employment purposes or shall have resources to direct client to this information. CRA shall advise client to consult their legal counsel regarding their specific legal responsibilities.	CRA shall provide written policy, procedure, or other documentation describing how/when clients are informed of client's legal responsibilities when using consumer reports for employment purposes and when/how clients are advised to consult their legal counsel regarding client's specific legal responsibilities. CRA shall also provide copy of document used to inform client or their legal responsibilities.	CRA shall present written procedure for informing client of client's legal responsibilities and advising client to consult with client's legal counsel. CRA shall make available the person responsible for retaining these 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 regarding client's legal responsibilities, be able to access current copy of documentation, <b>AND/OR</b> CRA employees shall identify person/s to address legal topics.	CRA shall inform clients of legal responsibilities and advise clients to 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.
<b>3.2 Client Required Documents</b>			

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
<p>CRA shall provide guidance and/or sample documents which are needed to meet legal requirements regarding employer's procurement and use of consumer reports.</p>	<p>CRA shall provide written policy, procedure, or other documentation describing how/when clients are provided with guidance and/or sample documents to meet legal requirements in the procurement and use of consumer reports. CRA shall also provide copy of document used to inform client or their legal responsibilities. If CRA provides sample documents, such documents shall also be provided.</p>	<p>CRA shall present documentation describing how/when guidance and/or sample documents are provided, guidance document/s which are provided, and any sample documents which are provided. CRA shall make available the person responsible for providing client guidance and sample documents. If interviewed, CRA employees shall demonstrate knowledge of client-required documents, be able to access current copy of documentation, <b>AND/OR</b> CRA employees shall identify person/s to address such topics.</p>	<p>CRA shall guide clients to appropriate source and/or shall provide samples of documents which are required for client to procure and use consumer reports. These currently 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.)</p>
<p><b>3.3 Truth in Advertising</b> CRA shall clearly communicate to clients the nature of the original source, limitations, variables affecting the information available and scope of information provided by each product.</p>	<p>CRA shall provide written policy, procedure, or other documentation describing how/when clients are provided with information that clearly describes the composition of each product, information source/s used for each 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 product disclosure, all personally identified information shall be redacted.</p>	<p>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 product disclosure, all personally identified information shall be redacted and auditor will not retain copy. If interviewed, CRA employees shall demonstrate knowledge that product descriptions exist, where such descriptions are documented, <b>AND/OR</b> the person responsible for CRA's products.</p>	<p>Information disclosed regarding 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. Disclosure of information source, type of source, scope of search, and search methodology may be included in consumer reports.</p>
<p><b>3.4 Adverse Action</b> CRA shall advise 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 advise client that they should consult their legal counsel prior to taking adverse action.</p>	<p>CRA shall provide written policy, procedure, or other documentation describing how/when clients are informed of client's legal responsibilities regarding adverse action when using consumer reports for employment purposes. CRA shall also provide copy of document used to inform client of Adverse Action requirements and such document shall include advising client to consult with legal counsel regarding adverse action.</p>	<p>CRA shall present written procedure for informing client of client's legal responsibilities regarding adverse action and advise 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, <b>AND/OR</b> CRA employees shall identify person/s to address such topics.</p>	<p>CRA may inform clients of legal responsibilities 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.</p>
<p><b>3.5 Legal Counsel</b></p>			

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
<p>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.</p>	<p>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.</p>	<p>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, <b>AND/OR</b> CRA employees shall identify person/s to address legal topics.</p>	<p>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.</p>
<p><b>3.6 Understanding Consumer Reports</b></p>			
<p>CRA shall provide guidance to client on how to order, retrieve, read and understand consumer reports provided by the CRA.</p>	<p>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.</p>	<p>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, <b>AND/OR</b> CRA employees shall identify person/s to address such topics.</p>	<p>CRA may provide information to clients regarding how to order, retrieve, read, and understand 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.</p>
<p><b>3.7 Information Protection</b></p>			
<p>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.</p>	<p>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.</p>	<p>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, <b>AND/OR</b> CRA employees shall identify person/s to address such topics.</p>	<p>CRA shall inform client 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 authorized 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.</p>
<p><b>Researcher and Data Standards</b></p>			
<p><b>4.1 Public Record Researcher Agreement</b></p>			

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
<p>CRA shall require a signed agreement from all utilized 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, reinvestigation requirements and other obligations as furnishers of information under the federal FCRA.</p>	<p>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 agreement requirements of Clause 4.3.)</p>	<p>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. 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.</p>	<p>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)</p>
<p><b>4.2 Vetting Requirement</b></p>			
<p>CRA shall have procedures in place to vet or qualify new public record researchers.</p>	<p>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.</p>	<p>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.</p>	<p>The vetting records should 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 "NAPBS PROVIDER GUIDELINES."</p>
<p><b>4.3 Public Record Researcher Agreement</b></p>			
<p>CRA shall require public record researcher to agree in writing that they will conduct research in compliance with all 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.</p>	<p>CRA shall provide written policy, procedure, or other written documentation describing how/when/where the signed agreement is obtained from and retained for all current public record researchers. CRA shall also provide copy of current agreement. (Note: This agreement may be incorporated in or an appendix to the "Public Record Researcher Agreement" described in Clause 4.1.)</p>	<p>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 retaining these agreements and auditor may ask to see (but not retain a copy of) signed agreements from one or more public record researchers. (Note: This agreement may be part of the "Public Record Researcher Agreement" described in Clause 4.1.) If interviewed, CRA employees responsible for working with public record researchers shall demonstrate understanding of agreement 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.</p>	<p>The document in which the Public Record Researcher agrees to the provisions in this clause 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 agreement may be part of the "Public Record Researcher Agreement" described in Clause 4.1.)</p>
<p><b>4.4 Errors and Omissions Coverage (E&amp;O)</b></p>			

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
<p>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.</p>	<p>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&amp;O coverage for uninsured/underinsured public record researchers.</p>	<p>CRA shall present written procedure for obtaining proof of public record researcher's E&amp;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&amp;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&amp;O requirement prior to utilizing services of public record researcher OR technology shall prevent utilization of public record researcher by CRA employees until CRA</p>	<p>The E&amp;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.</p>
<b>4.5 Information Security</b>			
<p>CRA shall provide a secure means by which public record researchers will receive orders and return search results.</p>	<p>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.</p>	<p>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.</p>	<p>Security procedures for personally identifiable information should include, but are not limited to: 1) all transmissions should be 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.</p>
<b>4.6 Auditing Procedures</b>			
<p>CRA shall maintain auditing procedures for quality assurance in regard to their active public record researchers.</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>
<b>4.7 Identification Confirmation</b>			
<p>CRA shall have procedures in place to confirm the identity of a consumer who is the subject of a record prior to reporting adverse information. If CRA is unable to confirm the identity of a consumer, CRA shall have procedures in place to notify client of any adverse information that is reported as a "Name Match Only" if CRA reports such record.</p>	<p>CRA shall provide written policy, procedure, or other written documentation describing the requirement to and method used to confirm the identity of the consumer who is the subject of a record prior to reporting such record to CRA client and how such information is handled if confirmation cannot be made.</p>	<p>CRA shall present written documentation for confirming identity of consumer prior to reporting adverse information and how such information is handled if confirmation cannot be made. CRA shall make available the person responsible for such identification confirmation. CRA employees responsible for such identification shall demonstrate knowledge of identification requirement and be able to access current documentation.</p>	<p>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 "Name Match Only" if CRA reports based on single identifier.</p>
<b>4.8 Jurisdictional Knowledge</b>			

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 a qualified individual(s) or position(s) within the organization responsible for understanding court terminology, as well as understanding the various jurisdictional court differences.	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 CRAs. CRA Court/Jurisdictional Knowledge 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 CRA Court/Jurisdictional Knowledge Leader.	CRA shall provide evidence of qualifications by presenting resume, educational credentials, experience, and/or other documentation.	N/A
<b>Verification Service Standards</b>		<b>DEFINITION:</b> 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 5.9) 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. As used in Clause 5.9, outsourcing criminal record checks to public record field researchers <b>ARE NOT</b> considered "Outsourced Verification Services."	
<b>5.1 Verification Accuracy</b> CRA shall have procedures in place to reasonably ensure accuracy and thoroughness 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 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.
<b>5.2 Current Employment</b>			

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 only contact consumer's current employer when authorized by client and/or consumer.	CRA shall provide written policy, procedure, or other documentation used to ensure consumer's current employer is contacted only when consumer has provided explicit authorization.	CRA shall make available to auditor tools or systems used (except actual personally identifiable information) to demonstrate procedures in place to prevent unauthorized contact with current employer. If interviewed, CRA employees responsible for verification of current employment shall demonstrate knowledge of authorization requirement and describe methodology by which they receive learn about such requirement. CRA employees responsible for current employer contact shall be able to access current copy of documentation, <b>AND/OR</b> 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 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 contacted only with authorization include, but are not limited to: 1) authorization provided on employment application, 2) explicit authorization provided within Disclosure/Authorization signed by consumer, <b>AND/OR</b> 3) technology shall prevent verification of current employment by CRA employees until CRA Leader has so enabled.
<b>5.3 Diploma Mills</b>			
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 diploma 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, <b>AND/OR</b> 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
<b>5.4 Procedural Disclosures</b>			
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 methodology documentation 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, <b>AND/OR</b> the person responsible for	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.
<b>5.5 Verification Databases</b>			

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
<p>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.</p>	<p>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.</p>	<p>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, <u>AND/OR</u> utilize technology to control the addition or deletion of information in the database/s.</p>	<p>This clause particularly addresses "resellers" of consumer information, such as Talx, National Student Clearinghouse, and credit bureaus. 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. In addition, CRA's who are resellers will likely utilize significant technological tools and systems to control the accuracy of information added to or deleted from database/s.</p>
<p><b>5.6 Use of Stored Data</b></p>			
<p>If CRA provides investigative consumer reports from stored data, CRA shall have procedures in place to ensure they do 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.</p>	<p>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.</p>	<p>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, <u>AND/OR</u> technology shall prevent utilization of stored adverse data which is older than 90 days.</p>	<p>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.</p>
<p><b>5.7 Documentation of Verification Attempts</b></p>			
<p>CRA shall have procedures in place to record all attempts made, and the result of each attempt, in completing all verification services.</p>	<p>CRA shall present written policy, procedure, or other written documentation used to ensure that all attempts made to verify information are fully documented.</p>	<p>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, <u>AND/OR</u> technology shall automatically capture attempts to verify and related information.</p>	<p>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.</p>
<p><b>5.8 Outsourced Verification Services</b></p>			

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
<p>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.</p>	<p>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.</p>	<p>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 Leader has enabled</p>	<p>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.</p>
<p><b>5.9 Conflicting Data</b> 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.</p>	<p>CRA shall provide written policy, procedure, or other documentation describing how conflicting data, when received within 120 days of report completion and as a direct result of original inquiry, is provided to client who originally ordered such report.</p>	<p>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.</p>	<p>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.</p>
<p><b>5.10 Professional Conduct</b> CRA shall train all employees on procedures for completing verification work in a professional manner.</p>	<p>CRA shall provide written policy, procedure, or other documentation which instructs CRA employees to complete verification work in a professional manner.</p>	<p>CRA shall make available to auditor any materials used to train CRA employees on professionalism when conducting verification work. If interviewed, CRA employees who conduct such verification work shall describe training which was received.</p>	<p>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.</p>
<p><b>5.11 Authorized Recipient</b> 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.</p>	<p>CRA shall provide written policy, procedure, or other documentation used to require that verification requests are directed to authorized recipients.</p>	<p>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.</p>	<p>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.</p>

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
<b>Miscellaneous Business Practices</b>			
<b>6.1 Character</b>			
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 accredited 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.
<b>6.2 Insurance</b>			
CRA shall maintain errors and omissions insurance or self-insure in a manner compliant with its state's insurance requirements.	CRA shall provide signed document affirming that CRA maintains errors and omissions insurance, the dollar amount of the insurance, and that said dollar amount complies with state requirements if such requirements exist.	CRA shall present to auditor copy of insurance requirements in the CRA's state of incorporation and insurance declaration page demonstrating that coverage meets state requirements. If the state does not have defined requirements, the CRA shall provide affirmation from CRA's insurance agent or legal counsel that: 1) no such requirements exist, and 2) CRA has errors and omissions insurance.	The E&O insurance should be in force. No specific amount is required but a minimum of two million in coverage is recommended.
<b>6.3 Client Authentication</b>			
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 authenticating 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.
<b>6.4 Vendor Authentication</b>			

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 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 authenticating 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 CRA's, a signed agreement between the vendor and CRA will suffice as authentication. Such vendors include but are not limited to: Experian, Equifax, TransUnion, Talx, National Student Clearinghouse, Softech, ADR, 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.
<b>6.5 Consumer Authentication</b>			
CRA shall have a procedure to identify and authenticate all consumers prior to disclosing consumer reports or other consumer information. The procedure shall require the CRA to maintain written records regarding the information used to identify each consumer who receives consumer reports or other consumer information	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 identification, how CRA representative confirms identify of consumer, and where record of authentication 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.
<b>6.6 Document Management</b>			
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 FCRA.
<b>6.7 Employee Certification</b>			
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

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
<p><b>6.8 Worker Training</b> CRA shall provide training to all workers on confidentiality, security and legal compliance practices of the CRA.</p>	<p>CRA shall provide written policy, procedure, or other documentation which describes the requirement for and methodology used to train CRA employees on the confidentiality, security, and legal compliance procedures of the CRA.</p>	<p>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.</p>	<p>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.</p>
<p><b>6.9 Visitor Security</b> CRA shall utilize a visitor security program to ensure visitors do not have access to consumer information.</p>	<p>CRA shall provide written policy, procedure, or other documentation which describes the visitor security program and how visitors are prevented from accessing consumer information.</p>	<p>CRA shall present written procedure for ensuring visitor security which prevents access to consumer information. CRA shall make available the person 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.</p>	<p>Visitor security policy must include method/s which 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.</p>
<p><b>6.10 Employee Criminal History</b> 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.</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>
<p><b>6.11 Quality Assurance</b> CRA shall have procedures in place to reasonably ensure the accuracy and quality of all work product.</p>	<p>CRA shall provide written policy, procedure, or other documentation describing the methods used to reasonably ensure the accuracy and quality of all work product.</p>	<p>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.</p>	<p>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.</p>
<p><b>6.12 Responsible Party</b></p>			

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
<p>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®.</p>	<p>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.</p>	<p>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 <u>OR</u> shall provide a signed affidavit 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.</p>	<p>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.</p>
<p><i>Miscellaneous Notes: Concepts of "Opportunity for Improvement" (OFI) and "Controlled Document"</i></p>			