

DRAFT
FOR DISCUSSION ONLY

CRIMINAL RECORDS ACCURACY ACT

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

October 23 – 24, 2015 Drafting Committee Meeting

Copyright © 2015
By
NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

The ideas and conclusions set forth in this draft, including the proposed statutory language and any comments or reporter's notes, have not been passed upon by the National Conference of Commissioners on Uniform State Laws or the Drafting Committee. They do not necessarily reflect the views of the Conference and its Commissioners and the Drafting Committee and its Members and Reporter. Proposed statutory language may not be used to ascertain the intent or meaning of any promulgated final statutory proposal.

October 5, 2015

DRAFTING COMMITTEE ON CRIMINAL RECORDS ACCURACY ACT

The Committee appointed by and representing the National Conference of Commissioners on Uniform State Laws in preparing this Act consists of the following individuals:

ROBERT J. TENNESSEN, 2522 Thomas Ave. S., Minneapolis, MN 55405, *Chair*

W. MICHAEL DUNN, P.O. Box 3701, 1000 Elm St., Manchester, NH 03105

MARK F. GLASER, 54 State St., 6th Floor, Albany, NY 12207

ERIC HOUGLAND, Texas Legislative Council, P.O. Box 12128, Austin, TX 78711-2128

JAMES C. KENNEDY, Massachusetts House of Representatives, State House, Room 139,
Boston, MA 02133

THEODORE C. KRAMER, 42 Park Pl., Brattleboro, VT 05301

JOHN J. MCAVOY, 3110 Brandywine St. NW, Washington, DC 20008

LOUISE M. NADEAU, Legislative Commissioners' Office, Connecticut General Assembly,
Legislative Office Bldg., Room 5500, Hartford, CT 06106-1591

ANNE H. REIGLE, Court of Common Pleas, Kent County Courthouse, 38 The Green, Dover,
DE 19901-3602

JACOB T. RODENBIKER, McKenzie County State's Attorney, 201 5th St. NW, Suite 550,
Watford City, ND 58854

MICHAEL S. SCHWOYER, Pennsylvania House of Representatives, Room 423, Main Capitol
Building, Harrisburg, PA 17120

BRANDON C. SHAFFER, 1154 Twin Peaks Cir., Longmont, CO 80503

SAMUEL A. THUMMA, Arizona Court of Appeals, State Courts Bldg., 1501 W. Washington
St., Phoenix, AZ 85007

RUSSELL G. WALKER, P.O. Box 2422, Jamestown, NC 27282

STEVEN L. CHANENSON, Villanova University School of Law, 299 N. Spring Mill Rd.,
Villanova, PA 19085, *Reporter*

JORDAN M. HYATT, Drexel University, Department of Criminology & Justice Studies, 3141
Chestnut Street, 217 PSA Building, Philadelphia, PA 19104, *Associate Reporter*

EX OFFICIO

RICHARD T. CASSIDY, 100 Main St., P.O. Box 1124, Burlington, VT 05402, *President*

H. LANE KNEEDLER, Office of the Attorney General of Virginia, 900 East Main St.,
Richmond, VA 23219, *Division Chair*

AMERICAN BAR ASSOCIATION ADVISORS

STEVE SALTZBURG, George Washington University Law School, 2000 H St. NW,
Washington, DC 20052-0026, *ABA Advisor*

MICHAEL AISENBERG, 7515 Colshire Dr., MS T320, McLean, VA 22102-7538, *ABA Section
Advisor*

EXECUTIVE DIRECTOR

LIZA KARSAI, 111 N. Wabash Ave., Suite 1010, Chicago, IL 60602, *Executive Director*

Copies of this Act may be obtained from:

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS
111 N. Wabash Ave., Suite 1010
Chicago, Illinois 60602
312/450-6600
www.uniformlaws.org

CRIMINAL RECORDS ACCURACY ACT

TABLE OF CONTENTS

SECTION 1. SHORT TITLE. 1

SECTION 2. DEFINITIONS. 1

SECTION 3. APPLICABILITY. 5

SECTION 4. SCOPE. 5

SECTION 5. DUTIES AND AUTHORITY OF CRIMINAL JUSTICE AGENCY FOR
CRIMINAL HISTORY RECORD INFORMATION. 6

SECTION 6. CRIMINAL JUSTICE AGENCY COLLECTION AND USE OF
INTELLIGENCE INFORMATION AND INVESTIGATIVE INFORMATION. 11

SECTION 7. DUTIES AND AUTHORITY OF THE CENTRAL REPOSITORY. 12

SECTION 8. SECURITY REQUIREMENTS FOR CRIMINAL JUSTICE AGENCIES AND
CENTRAL REPOSITORY. 21

SECTION 9. SUBJECT’S RIGHT OF ACCESS, REVIEW, CHALLENGE, CORRECTION,
AND APPEAL. 21

SECTION 10. MANDATORY INDEPENDENT ANNUAL AUDIT. 24

SECTION 11. SANCTIONS AND REMEDIES. 25

SECTION 12. DUTIES AND AUTHORITY OF [ATTORNEY GENERAL]. 26

SECTION 13. UNIFORMITY OF APPLICATION AND CONSTRUCTION. 27

SECTION 14. REPEALS; CONFORMING AMENDMENTS. 27

SECTION 15. EFFECTIVE DATE. 27

1 **CRIMINAL RECORDS ACCURACY ACT**

2 **SECTION 1. SHORT TITLE.** This [act] may be cited as the Criminal Records
3 Accuracy Act.

4 **SECTION 2. DEFINITIONS.** In this [act]:

5 (1) “Administration of criminal justice” means activities directly involving with the
6 prevention, control or reduction of crime, or the apprehension, detention, pre-trial release, post-
7 trial release, prosecution, adjudication, correctional supervision or rehabilitation of accused
8 persons, or criminal offenders.

9 (2) “Attorney General” mean the Attorney General of this state.

10 (3) “Audit” means the process of reviewing compliance with applicable state and federal
11 laws and regulations related to the accuracy, security, and privacy of criminal history record
12 information.

13 (4) “Biometric identifying information” means distinctive attributes of an individual,
14 including fingerprints used for identification.

15 (5) “Central repository” means the single, centralized entity for collection, compilation,
16 storage, maintenance, and dissemination of criminal history record information operated by the
17 [office, department, or State Police]. For the purpose of this [act], the central repository is not a
18 criminal justice agency.

19 (6) “Criminal history record information” means information collected by criminal justice
20 agencies or the central repository consisting of identifiable descriptions, including biometric
21 identifying information, and notations of reportable events. The term does not include
22 intelligence information or investigative information.

23 (7) “Criminal justice agency” means the Office of the Attorney General, any court with

1 criminal jurisdiction, or subdivision of this state authorized to perform as one of its principal
2 functions the administration of criminal justice and which allocates a substantial portion of its
3 budget to that function. The term includes an organized state or municipal police department,
4 local detention facility or department, county, regional or state correctional facility or
5 Department, probation agency, [district or prosecuting] attorney, parole board, pardon board,
6 juvenile detention facility, and any agency or subunit as declared by the [Attorney General] to be
7 a criminal justice agency.

8 (8) "Dissemination" means oral, written, or electronic transmission or other disclosure of
9 criminal history record information to a person other than the central repository or the criminal
10 justice agency that maintains the information.

11 (9) "Dissemination log" means a listing of every request for, and dissemination of,
12 criminal history record information or intelligence information or investigative information,
13 indicating the information requested, information disseminated, each person and associated
14 address relating to the request or dissemination, the date of the request or dissemination, and the
15 purpose for which it was requested or disseminated. The dissemination log is separate and
16 distinct from the criminal history record information, intelligence information, or investigative
17 information itself. Each entry in a dissemination log must be maintained for at least five years.

18 (10) "Expunge" means remove information pursuant to statute or court order so there is
19 no indication the information existed.

20 (11) "Intelligence information" means information about the habits, practices,
21 characteristics, possessions, associations, or financial status of an individual compiled in an
22 effort to anticipate, prevent, monitor, investigate or prosecute criminal activity.

23 (12) "Investigative information" means information assembled as a result of the

1 performance of an inquiry, formal, or informal, into a criminal incident or an allegation of
2 criminal wrongdoing, and may include modus operandi information.

3 (13) "Person" means an individual, estate, business or nonprofit entity, public
4 corporation, government or governmental subdivision, agency, or instrumentality, or other legal
5 entity.

6 (14) "Registry to prevent fraud victimization" means an independent database comprised
7 of identifying information voluntarily provided by victims of identity theft and/or fraud, persons
8 whose names or other identifying characteristics are similar to other persons who have criminal
9 history records, or persons concerned about such potential victimization and designed to prevent
10 the erroneous creation or modification of Criminal History Record Information.

11 (15) "Reportable event" means any of the following occurrences concerning a person
12 suspected of, arrested for, or charged with a criminal offense, including felonies and
13 misdemeanors but excluding petty offenses, [noncriminal or summary] traffic violations, and
14 offenses adjudicated under the [Juvenile Court Act]:

15 (A) an arrest;

16 (B) a disposition after an arrest without the filing of a formal criminal charge;

17 (C) the filing of a formal criminal charge;

18 (D) the disposition of a formal criminal charge, including a diversion, dismissal,
19 indefinite postponement, mistrial, acquittal, conviction, sentence imposed, and modification,
20 reversal, or revocation of the disposition;

21 (E) commitment after conviction to or release from a place of detention or
22 custodial supervision;

23 (F) commencement or conclusion of noncustodial supervision by a Criminal

1 Justice Agency;
2 (G) completion of sentence;
3 (H) an expungement or sealing; and
4 (I) a finding of mental incompetence by a court of this state at any stage of a
5 judicial proceeding.

6 (16) “Repository” means an entity operated by a criminal justice agency which collects,
7 compiles, maintains, or disseminates criminal history record information.

8 (17) “Sealing” means a court order that prohibits public release of criminal history record
9 information.

10 (18) “State” means a state of the United States, the District of Columbia, Puerto Rico, the
11 United States Virgin Islands, or any other territory or insular possession subject to the
12 jurisdiction of the United States. The term includes a federally recognized Indian tribe.

13 (19) “Subject” means an individual who is the subject of criminal history record
14 information.

15 Discussion Notes

16
17 *Defined terms, not substance.* The style rules of the Uniform Law
18 Commission call for consolidation of definitions for terms that recur throughout an
19 act into a single section early in the act. A definition for a term that appears in only
20 one section should be located in that section. Provisions that state a definition must
21 be definitional only, with the substance pertaining to the term addressed
22 separately.

23
24 *Biometric identifying information.* The definition of “biometric identifying
25 information” is designed to allow the act to adapt automatically as technology
26 evolves. Right now, fingerprints are the gold standard for ensuring that a
27 particular person is linked to arrest and disposition information. That may change
28 and the definition should be able to accommodate such changes. In this case, we
29 consider DNA information to fall outside the scope of biometric identifiers, though
30 this is not made explicit in the text.

1 *Central repository.* The definition of “central repository” leaves to the
2 adopting state whether this is a police function, often through the state police, or an
3 independent function. Given the central repository’s coordinating role, the
4 definition does require the central repository to be independent from criminal
5 justice agencies or other repositories.

6
7 *Criminal justice agency.* The definition of “criminal justice agency” is
8 intentionally broad. The goal is to widely distribute the duty to provide information
9 on “reportable events” – such as arrests, charges, and dispositions of all types – to
10 the central repository. This also allows for the collection and inclusion of
11 reportable event and identification data throughout the process of adjudication and
12 punishment, thereby allowing for multiple instances to collect data and resolve
13 issues.

14
15 *Reportable event.* The definition of a “reportable event” is designed to capture
16 all of the significant moments in the life of a criminal case that future actors in the
17 criminal justice system would want to know about that defendant and that case.
18 Though the nomenclature may vary by jurisdiction, these are almost universal in
19 their presence and importance.

20
21 **SECTION 3. APPLICABILITY.** This [act] applies to persons within this state and to
22 any criminal justice agency of this state or its political subdivisions which collects, maintains,
23 modified, disseminates, or receives criminal history record information.

24 **SECTION 4. SCOPE.**

25 (a) General rule. Except for the provisions of Section 5 (relating to Duties and Authorities
26 of Criminal Justice Agencies), Section 8 (relating to Security Requirements for Criminal Justice
27 Agencies and the Central Repository) and Section 9 (relating to Right to Access, Review,
28 Challenge and Correction), nothing in this [act] may be construed to apply to:

29 (1) any documents or records prepared by, or maintained by, or filed in any court
30 of this state; or

31 (2) announcements of executive clemency made by the [Governor] or the
32 [Governor’s] designee.

33 (b) Court dockets. Court dockets, court files, and information contained therein shall, for

1 purposes of this [act], be considered public records.

2 **Discussion Notes**

3 *Public records.* This section is designed to ensure that information in court
4 dockets and files remain public records. Through the exemptions in paragraph (a),
5 however, it does so while still requiring that courts submit information about
6 reportable events to the central repository. We have some concerns about
7 separation of powers, but believe that existing legislation in certain jurisdictions
8 requires judicial participation. If the members of the drafting committee are
9 concerned about this point, we can explore it further before circulating the next
10 draft.

11
12 **SECTION 5. DUTIES AND AUTHORITY OF CRIMINAL JUSTICE AGENCY**
13 **FOR CRIMINAL HISTORY RECORD INFORMATION.**

14 (a) Authority to Disseminate Generally. A criminal justice agency may only disseminate
15 criminal history record information as provided in this [act].

16 (b) Mandatory Duty to Collect Biometric Identifying Information. The following
17 provisions govern the collection of fingerprints and other biometric identifying information:

18 (1) An arresting criminal justice agency must collect biometric identifying
19 information in the manner and form directed by the central repository, of a person arrested for a
20 felony or misdemeanor [or summary offense that becomes a misdemeanor on a second arrest
21 after conviction of the summary offense], and must forward that information to the central
22 repository, in the manner and form directed by the central repository, not later than 48 hours after
23 the arrest.

24 (2) If a defendant charged with a felony or misdemeanor [or summary offense that
25 becomes a misdemeanor on a second arrest after conviction of the summary offense] by
26 complaint, information, or indictment is not arrested and instead appears in court pursuant to
27 summons, the court must order the defendant to report to the local municipal police department
28 or [state] police not later than two business days after the order and permit the police to collect

1 biometric identifying information as prescribed by the central repository. The police department
2 must then forward that information to the central repository, in the manner and form directed by
3 the central repository, not later than 48 hours after collection.

4 (3) During the investigation, adjudication and correctional processes, the head of
5 each criminal justice agency responsible for the arrest, prosecution, adjudication, sentencing,
6 supervision, or custody of a person for a felony or misdemeanor [,or summary offense which
7 becomes a misdemeanor on a second arrest after conviction of that summary offense,] must
8 determine whether biometric identifying information as prescribed by the central repository, has
9 previously been collected for that person and forwarded to the central repository in the manner
10 and form directed by the central repository.

11 (4) If any head of a criminal justice agency responsible for the arrest, prosecution,
12 adjudication, sentencing, supervision, or custody of a person for a felony or misdemeanor [,or
13 summary offense which becomes a misdemeanor on a second arrest after conviction of that
14 summary offense,] determines, pursuant to paragraph 3 above, that biometric identifying
15 information had not been collected and forwarded to the central repository, the head of the
16 criminal justice agency shall collect biometric identifying information as prescribed by the
17 central repository not later than 72 hours after making that determination and forward that
18 information to the central repository not later than 48 hours after collection.

19 (c) Mandatory Duty to Report Reportable Events. A criminal justice agency must collect,
20 in the manner and form directed by the central repository, information on reportable events with
21 which the criminal justice agency was involved. A criminal justice agency must then submit that
22 information, in the manner and form directed by the central repository, to the central repository
23 not later than 72 hours after the reportable event.

1 (d) Duty of Security. A criminal justice agency must maintain all criminal history record
2 information in a secure manner as provided in Section 8.

3 (e) Duty of Accuracy. A criminal justice agency must maintain complete and accurate
4 criminal history record information and report this information as required by this [act] or other
5 statutes and regulations. A repository must establish effective procedures, in compliance with
6 regulations adopted by the [Attorney General], to create and store complete and accurate criminal
7 history record information.

8 (f) Duty to Correct Inaccurate Information. Regardless of the manner of discovery and
9 the person who discovered it, not later than 15 days after the becoming aware of inaccurate
10 criminal history record information, the criminal justice agency that reported the inaccurate
11 information must:

12 (1) correct its own records; and

13 (2) disseminate a notice to the central repository and all other persons that
14 received the inaccurate information as reflected in the required dissemination logs about the
15 inaccuracy and the required correction.

16 (g) Authority to Disseminate to Criminal Justice Agencies. A criminal justice agency
17 may disseminate criminal history record information to another criminal justice agency upon a
18 request in connection with the requesting agency's duties. A criminal justice agency must create
19 and maintain a dissemination log concerning disseminations of criminal history record
20 information to another criminal justice agency.

21 (h) Duty to Disseminate to Subjects. A criminal justice agency must disseminate criminal
22 history record information to the subject of that information on request of the subject or the
23 subject's designee, and at a reasonable cost consistent with regulations adopted by the [Attorney

1 General]. If criminal history record information sought by the subject is maintained by a
2 criminal justice agency in a record also containing investigative information, or intelligence
3 information, or other nonpublic information, the agency may remove that information and
4 disseminate only the criminal history record information. If the agency identifies no criminal
5 history record information, it must indicate to the subject or the subject’s designee that no
6 relevant records were identified and the date of the search. A criminal justice agency must create
7 and maintain a dissemination log concerning disseminations of criminal history record
8 information to a subject.

9 **Discussion Notes**

10 *Mandatory duty to collect biometric identifying information.* We believe that
11 Section 5(b) is one of the most important requirements in the act. Biometric
12 identifying information, in the form of fingerprints, is the gold standard for positive
13 identification for law enforcement purposes. If this information is not used to link
14 an arrest to a charge to a disposition, significant inaccuracies may and do result. In
15 most cases, close matches using name and date of birth are the alternative. This is
16 a clear and common source of inaccuracies – both in the failure to link related
17 reportable events and in the misidentification of the subject. Section 5(b) puts the
18 primary responsibility for this task on the arresting criminal justice agency, which
19 will typically be the police. In our preliminary explorations, the lack of collection at
20 the “front line” of processing was a significant impediment. In some jurisdictions,
21 this appears to be unrelated to funding for equipment, and instead turns on the
22 enforcement of mandatory collection procedures. *See, e.g., Jeffrey Benzing,*
23 *Fingerprint Hearing: Best and Worst Pa. Counties Have Same Equipment,* available
24 at
25 http://www.pennlive.com/midstate/index.ssf/2014/07/fingerprint_hearing_best_and_w.html
26 (July 23, 2014).

27
28 *Duty of other criminal justice agencies.* If the arresting agency fails to obtain
29 fingerprints, the act provides a backstop by requiring other, functionally
30 downstream, actors in the criminal justice system to fingerprint the subject. We
31 believe that this “belt-and-suspenders approach” is warranted given the wide
32 variation of fingerprint compliance rates between and within states. For example,
33 we were told that in one large state, there are tens, if not hundreds, of thousands of
34 essentially orphaned files in the central repository because disposition information
35 cannot be definitively linked by fingerprint to a person. Furthermore, in that state,
36 the state prison receiving center felt the need to install a livescan machine (a

1 common biometric data collection station) because of the number of sentenced
2 offenders arriving without fingerprints in the system. At the same time, this
3 jurisdiction has a nearly uniform collection provision for fingerprint information,
4 highlighting the creation and reinforcement of need for multiple opportunities to
5 obtain these key data.

6
7 *Duty to report reportable events.* Section 5(c) requires criminal justice
8 agencies to submit information on reportable events – such as arrests, charges,
9 convictions, sentences, commitments, etc. – with which they were involved to the
10 central repository. If followed, this mandate should go a long way towards solving
11 the problem of missing dispositions. We again took a “belt-and-suspenders
12 approach” by putting this responsibility broadly on multiple actors, even if that
13 means some duplicative reporting to the central repository. Given the large and
14 growing use of electronic records, this should not be burdensome on the criminal
15 justice agencies and may help to reduce inaccuracies. Some additional effort may be
16 necessary to define the scope of involvement necessary to trigger this duty, but the
17 self-reinforcing nature of this collection system remains a key component of this
18 draft of the act.

19
20 *Duty to correct inaccuracies.* Section 5(f), which has a corollary for the
21 central repository as well, requires the criminal justice agency that learns of an
22 inaccuracy – regardless of how it learns of it – to fix it in its own records and to pass
23 along the corrected information to whomever it has provided the inaccurate
24 information. That latter process is facilitated by the maintenance of dissemination
25 logs. Thoroughly tracking the information will allow for more effective correction,
26 as well as providing essential process data for the audit, discussed in Section 10.

27
28 *Authority to disseminate.* These provisions allow criminal justice agencies to
29 disseminate criminal history record information to other criminal justice agencies
30 and to the subject of the information upon request. The central repository, as part
31 of its duties, will set reasonable standards and procedures for this process, ensuring
32 a degree of uniformity in the requesting and dissemination processes.

33
34 These are some of the several provisions that call for implementing
35 regulations. We value the idea of checks and balances and thus want these
36 regulations – like the audits in Section 10 – to be controlled by an entity outside of
37 the day-to-day operation of the criminal record system. The central repository is a
38 perfectly appropriate entity to create operation rules, as in Section 5(b)(1) and
39 Section 7(h), and we certainly are not impugning the integrity of the individuals
40 within the criminal record system. This is simply a structural point. We typically
41 identified the Attorney General for this role because that official often has broad
42 “minister of justice” responsibilities within the criminal justice system. However,
43 we identified the Attorney General in brackets because we understand that this
44 official may not be the appropriate choice for every state.

1 **SECTION 7. DUTIES AND AUTHORITY OF THE CENTRAL REPOSITORY.**

2 (a) General Rule. The central repository must collect and maintain the criminal history
3 record information reported to it under this [act]. The central repository may only disseminate
4 criminal history record information as provided in this [act].

5 (b) Information from other Jurisdictions. The central repository may request, access and
6 store records relating to an offense committed in another jurisdiction. The records may include
7 federal summary criminal history information provided by the United States Department of
8 Justice and other information that would qualify as criminal history record information if
9 submitted by a criminal justice agency. For purposes of maintenance and dissemination,
10 information from another jurisdiction must be treated as if it were from this state.

11 (c) Duty of Accuracy. The central repository shall facilitate the creation and maintenance
12 of complete and accurate criminal history record information, by:

13 (1) establishing practices and procedures necessary to efficiently and as
14 automatically as possible resolve conflicts and missing data on the same incident or subject; and

15 (2) expunging criminal history record information pursuant to law or court order.

16 (d) Intelligence Information and Investigative Information Prohibited. The central
17 repository may not collect, maintain, or disseminate intelligence information or investigative
18 information. This prohibition does not preclude the collection of a name, word, number, phrase,
19 or other similar index key to serve as an index to investigative reports.

20 (e) Duty to Disseminate to Criminal Justice Agencies and Related Entities. The central
21 repository must:

22 (1) disclose criminal history record information to a criminal justice agency on
23 request by the agency for information sought in connection with the agency's duties.

1 (2) disclose criminal history record information to the Governor to aid in a
2 decision concerning an exercise of the power of pardon, reprieve, commutation or reduction of
3 sentence, executive clemency, or interstate extradition or rendition.

4 (3) disclose criminal history record information as constitutionally required or as
5 expressly required by a statute of [this state] or the United States.

6 (4) disclose criminal history record information to a criminal justice agency of
7 another state upon request for the information by the agency in connection with the agency's
8 duties if that state has enacted the provisions of [this act].

9 (5) disseminate criminal history record information to the Federal Bureau of
10 Investigation and United States Department of Justice as part of the state's participation in the
11 Interstate Identification Index System, National Fingerprint File, National Identification Index,
12 National Instant Criminal Background Check System Index, and related federal programs.

13 (f) Duty to Disseminate for Employment, Licensing or Certification Purposes.

14 (1) When directed by the law of the state or the United States, the central
15 repository must disseminate criminal history record information, including federal summary
16 criminal history information provided by the Federal Bureau of Investigation or the United States
17 Department of Justice, to a person for employment, licensing, or certification purposes, subject
18 to the following conditions:

19 (2) Before the central repository disseminates criminal history record information,
20 including federal summary criminal history information provided by the United States
21 Department of Justice, to a person for employment, licensing, or certification purposes as
22 directed by the laws of this state or the United States, it must determine whether the information
23 contains a disposition after an arrest without the filing of a formal criminal charge or a

1 disposition of a formal criminal charge for every arrest or charge. If disposition information is
2 missing, the central repository must first:

3 (A) make a good faith effort to determine the disposition of the arrest or
4 charge; and

5 (B) add that information to:

6 (i) the relevant records maintained by the central repository; and

7 (ii) the report or summary to be disseminated.

8 (3) Before the central repository disseminates criminal history record information,
9 including federal summary criminal history information provided by the United States
10 Department of Justice, to a person for employment, licensing, or certification purposes as
11 directed by the laws of this state or the United States, it must remove from the report or summary
12 to be disseminated all notations of arrests, charges, indictments or other information relating to
13 the initiation of criminal proceedings where:

14 (A) eighteen months have elapsed after the date of arrest;

15 (B) no conviction has occurred; and

16 (C) no proceedings are pending seeking a conviction.

17 (4) When the central repository disseminates criminal history record information,
18 including federal summary criminal history information provided by the United States
19 Department of Justice, to a person for employment, licensing, or certification purposes as
20 directed by the laws of this state or the United States, it must send the same information to the
21 subject by certified United States mail directed to the subject's last known address in the central
22 repository's records and the subject's current address as obtained by, or provided to, the
23 requesting employment or licensing agency within 24 hours.

1 (g) Duty to Correct Inaccurate Information. Regardless of the manner of discovery and
2 the person who discovered it, not later than 15 days after the becoming aware of inaccurate
3 criminal history record information, the central repository must:

4 (1) correct its own records; and

5 (2) notify all criminal justice agencies that submitted information about reportable
6 events concerning the subject of the information inaccuracy and the required correction; and

7 (3) notify persons that received the inaccurate information as reflected in the
8 required dissemination logs, including the Federal Bureau of Investigation and United States
9 Department of Justice as part of the state's participation in the Interstate Identification Index
10 System, National Fingerprint File, National Identification Index, National Instant Criminal
11 Background Check System Index, and related federal programs.

12 (h) Duty and Authority to Establish Procedures. The central repository must establish
13 effective procedures, in compliance with regulations adopted by the [Attorney General], to
14 ensure the completeness and accuracy of criminal history record information. The central
15 repository must:

16 (1) specify the manner and form in which a criminal justice agency must submit
17 criminal history record information to the central repository concerning a reportable event,
18 including standards for biometric identifying information, to ensure that multiple pieces of
19 criminal history record information for the same subject are appropriately linked;

20 (2) develop and adopt procedures, standards, and forms for reporting and
21 exchanging information under this [act]; and

22 (3) adopt any other regulations necessary to carry out its duties under this [act].

23 (i) Authority to Disclose Anonymous Information. The central repository may

1 disseminate criminal history record information for statistical or research purposes, provided the
2 identity of the subject of the criminal history record information is not disclosed directly or
3 indirectly and the use of such information is subject to procedures established by the central
4 repository designed to implement this subsection.

5 (j) Duty to Provide Public Notice. The central repository must inform the public about the
6 existence, justification, usage, and accessibility of the criminal history record information
7 maintained by the central repository and other repositories. The central repository must also
8 provide public notice, updated at least every six months, concerning:

9 (1) the items of information that are used to retrieve and link criminal history
10 record information;

11 (2) the results of the annual audit and the status of any remediation efforts; and

12 (3) the requirements and forms required for individual access and review of
13 criminal history record information.

14 (k) Duty to Train. The central repository shall:

15 (1) provide regular training to criminal justice agencies throughout the state on
16 how to submit information about a reportable event and why the information is important to both
17 the administration of criminal justice and society.

18 (2) identify those criminal justice agencies and repositories not meeting minimum
19 standards under this [act] and provide them with remedial training.

20 (l) Duty to Create a Registry to Prevent Fraud Victimization.

21 (1) Responsibility to create a registry. The central repository must create and
22 maintain a registry to prevent fraud victimization.

23 (2) Submission requirements. The central repository must establish reasonable

1 requirements and procedures for inclusion in the registry identified in paragraph (1). Those
2 requirements must include collecting biometric identifying information from persons seeking to
3 be part of the registry.

4 (3) Eligibility for submission. An individual may voluntarily provide information
5 for consideration for inclusion the registry. After providing information sufficient to meet the
6 requirements provided in paragraph (2), an individual's name and information must be entered
7 into the registry.

8 (i) An individual denied inclusion in registry may seek relief under the
9 state [administrative procedures act] as a contested case.

10 (4) Documentation of enrollment. Not later than 14 days after entering an
11 individual in the registry, the central repository must issue a document to the individual
12 establishing that individual is a victim of identity theft, fraud or that the applicant is not an
13 individual with a similar name or identifying characteristics who has a criminal record.

14 (i) An individual who receives a document from the central repository
15 establishing that they are a victim of identity theft, fraud or not the individual with a similar
16 name or identifying characteristics may use the document to establish that fact.

17 (ii) The document provided by the central repository serves as prima facie
18 proof of that fact.

19 (5) Use of registry data. The central repository must not reveal information from
20 the registry except as specified in this act.

21 (6) The central repository must disclose information from the registry to a
22 criminal justice agency to prevent fraud victimization on request of a criminal justice agency and
23 when there is an indication that the identity information concerning a reportable event is

1 potentially inaccurate and not associated with the correct individual.

2 (i) A criminal justice agency, during the process of identifying an
3 individual who is the subject of reportable event, must submit the biometric identifying
4 information and/or identification data provided by the individual to the central repository for
5 comparison with information in the registry.

6 (ii) If the information provided matches, wholly or on part, any
7 information in the registry, the central repository must notify the criminal justice agency
8 immediately.

9 (iii) When there is a potential conflict or fraud, the criminal justice
10 agency must use biometric identifying information and any other identification methodologies
11 available to ensure the accurate identify of the subject of the reportable event prior to the creation
12 of any criminal history record information.

13 (7) Requirement to verify. Upon receiving information from the registry that the
14 identity information may be inaccurate or not associated with the correct individual or when an
15 individual produces a valid document from the central repository, a criminal justice agency must
16 use due diligence to accurately identify the subject in question.

17 (8) Limitation on use. A criminal justice agency must not use information from
18 the registry for any purpose other than to accurately identify the individual about whom it has
19 requested registry information, including the investigation or prosecution of any criminal or civil
20 matter.

21 (9) Sanctions for misuse. If information from the registry to prevent fraud
22 victimization is accessed for any reason other than those expressly permitted under this [act]:

23 (i) the information itself and any information acquired as a result must be

1 excluded from use in any criminal or civil matter;

2 (ii) the central repository must notify the individual whose information
3 was improperly obtained from the registry to prevent fraud victimization in writing within 2
4 business days;

5 (10) Security of registry. central repository must ensure the security of all
6 information in the registry to prevent fraud victimization. These protections must at least meet, ,
7 but may exceed, those provided in Section 8..

8 (11) Expiration of information.

9 (i) All information submitted to the registry to prevent fraud victimization
10 expires three years from the date of receipt unless the individual who provided the information
11 submits a notarized written request that the information be maintained for another three-year
12 period.

13 (ii) The central repository must permanently delete all expired information
14 from the registry to prevent fraud victimization within five days of its expiration.

15 (iii) After information in the registry to prevent fraud victimization has
16 expired, that information may only be restored to the registry to prevent fraud victimization
17 pursuant to a new submission.

18 (12) Removal of data. Upon receiving a notarized, written request from the
19 individual who voluntarily submitted information to the registry to prevent fraud victimization,
20 the central repository must permanently remove that information within five business days.

21 *Role of the central repository.* The central repository is the hub into and out
22 of which criminal history record information will flow. It serves this role, as it does
23 in many jurisdictions, for both intra-state and inter-state purposes. There are duty
24 of accuracy and correction provisions that are similar to the ones provided for
25 criminal justice agencies. The central repository is also the primary contact for
26 other states and the federal system, allowing it to serve as a clearing house for the

1 management of the universe of criminal history record information that may be fed
2 into the databases held within that jurisdiction.

3
4 *Role in employment checks.* The central repository’s primary function is to
5 act as the hub for criminal history record information used for criminal justice
6 purposes. There is, of course, a growing use of this information for mandated
7 employment, licensing and certification purposes. Section 7(f) addresses that role
8 directly. Accuracy concerns are heightened in this context. Paralleling efforts
9 considered to be successful by some in California, this section requires the central
10 repository to make a good faith effort to ensure that disposition information is
11 connected to arrests and charges. Without disposition information, Section 7(f)(3)
12 bars the disclosure of certain arrests more than 18 months old. After we drafted
13 Section 7(f)(3), Senator Grassley and others introduced the Sentencing Reform and
14 Corrections Act of 2015 (“SRCA”) on October 1, 2015. Section 213 of the SRCA is
15 entitled “Ensuring Accuracy of Federal Criminal Records;” we will review it more
16 closely and monitor its progress in the Congress before our next meeting. It is
17 worth noting for now, however, that pursuant to the SRCA certain arrests without
18 disposition information that are more than two years old could not be disseminated.
19 It may be worth considering, as a committee, if the SRCA approach more or less
20 desirable.

21
22 *Outreach to the public and criminal justice agencies.* Section 7(j) and 7(k)
23 assign the central repository educative and supportive roles. It will try to raise
24 public awareness about the importance of criminal history record information and
25 how individuals can access their records to check for accuracy. It will also have the
26 responsibility train criminal justice agencies and focus on those agencies that are
27 not reporting as required because those agencies present significant accuracy risks
28 to the entire system. We envision a system of web-based postings, webinars and
29 guidelines, though the central repository has the flexibility to conduct this outreach
30 in the manner determined to be effective in that jurisdiction.

31
32 *Registry to prevent fraud victimization.* Section 7(l), which is modeled in part
33 on a Minnesota provision, is designed to proactively help individuals who are the
34 victim of identity theft or believe that they may, be while also improving the
35 accuracy of the criminal record system more broadly. It allows for these individuals
36 to voluntarily provide information about themselves, including biometric identifying
37 information, to a restricted registry which would be used to verify whether a
38 particular person truly is the subject of a reportable event. We expand this
39 provision, including the provision of a verification letter, to include all individuals
40 who may seek to be proactive about limiting damaging errors in their own criminal
41 record. The documentation envisioned in Section 7(l)(4) should help a person
42 without a particular criminal record from suffering adverse consequences of being
43 confused with the person who actually has that record. At the same time, we
44 sought to balance these considerations with the burdens imposed on law

1 enforcement during the identity verification process(es).

2
3

SECTION 8. SECURITY REQUIREMENTS FOR CRIMINAL JUSTICE

4 **AGENCIES AND CENTRAL REPOSITORY.**

5 (a) General Rule. A criminal justice agency that collects, stores, or disseminates criminal
6 history record information, or intelligence information, or investigative information, and the
7 central repository must ensure the confidentiality and security of the information by:

8 (1) adopting procedures to reasonably protect locations where information is
9 maintained from theft, fire, sabotage, flood, wind or other natural or man-made disasters;

10 (2) ensuring that only authorized personnel have access to the information;

11 (3) selecting, supervising, training all personnel authorized to have access to the
12 information;

13 (4) ensuring that, where computerized data processing is employed, the equipment
14 for maintaining the information meets the computer security standards promulgated by the
15 [Attorney General]; and

16 (5) maintaining an index of all data breaches relating to the information for use by
17 the [Attorney General, State Auditor, Ombudsman, or Inspector General] under Section 10.

18 **SECTION 9. SUBJECT’S RIGHT OF ACCESS, REVIEW, CHALLENGE,**
19 **CORRECTION, AND APPEAL.**

20 (a) General Rule. A subject or a subject’s designee, after positive verification of identity
21 pursuant to implementing regulations under this [act], has the right to access, review, challenge,
22 correct, and appeal the accuracy and completeness of the subject’s criminal history record
23 information maintained by a repository or the central repository.

24 (b) Access and Review. A subject or a subject’s designee may, after properly submitting

1 a request, access and review a copy of the subject's criminal history record information without
2 undue delay for the purposes of challenge and correction.

3 (c) Challenge. A subject or the subject's designee may challenge the accuracy of the
4 subject's criminal history record information by specifying in writing the part of the criminal
5 history record information that is inaccurate and providing the correct information to repository
6 or central repository maintaining the information alleged to be inaccurate. This challenge must
7 be made pursuant to the state [administrative procedures act.]

8 (d) Review of challenge. The repository or the central repository has 45 days from the
9 date of receipt of the challenge to the accuracy of the information to conduct a review of a
10 challenge and has the burden of proving to [an administrative law judge] the accuracy of the
11 information by clear and convincing evidence. The [administrative law judge's] decision on the
12 challenge must include all information that formed the basis for the decision, including the
13 jurisdiction and docket number of any relevant court decision. If [the administrative law judge]
14 determines the challenge to be valid, the repository or central repository must:

15 (1) correct its own records;

16 (2) notify all persons that received the inaccurate information as reflected in the
17 required dissemination logs of both the inaccuracy and the required correction.

18 (3) notify the Federal Bureau of Investigation and the United States Department
19 of Justice of the inaccuracy in the information and the required correction;

20 (4) provide five corrected copies of the criminal history record information to the
21 subject or the subject's designee at no cost to the subject or the subject's designee; and

22 (5) provide the subject or the subject's designee with the names and addresses of
23 all persons to whom the inaccurate criminal history record information was disseminated within

1 the previous five years, and the dates of the disseminations.

2 (e) Appeals. If the [administrative law judge] rejects the challenge:

3 (1) The subject or the subject's designee may appeal the decision of the
4 [administrative law judge] to the [Attorney General] not later than 45 days after notification of
5 the decision by the [administrative law judge];

6 (2) The [Attorney General or the Attorney General's designee employed by the
7 Office of the Attorney General] must conduct a hearing de novo in accordance with the
8 state[administrative procedures act].

9 (3) If the [Attorney General or the Attorney General's designee employed by the
10 Office of the Attorney General] denies the challenge, the subject or the subject's designee may
11 appeal the denial to the [appellate] court not later than 45 days after the [Attorney General or the
12 Attorney General's designee employed by the Office of the Attorney General] notifies the
13 subject or the subject's designee of the denial. The [appellate] court will review the [Attorney
14 General or the Attorney General's designee employed by the Office of the Attorney General]
15 denial for abuse of discretion.

16 *Access, review, challenge, correction and appeal.* This section provides
17 individuals with robust rights to access and challenge the criminal history record
18 information about them for the explicit purpose of ensuring that all of the criminal
19 history record information managed by the state, regardless of its source, is correct
20 and up-to-date. The right to challenge under Section 9(c) is broad, but the state
21 administrative procedures act in place should be able to address abusive filers. Our
22 review indicates that most, if not all, jurisdictions already have procedures in place
23 to addresses matters of this nature. The first review would be resolved by an
24 administrative law judge, either internal to the entity subject to the challenge (e.g.,
25 the central repository) or otherwise as set forth in the state administrative
26 procedures act, with the burden on the government given its greater and easier
27 access to the official records. In response to an adverse ruling, the individual may
28 demand a *de novo* appeal to a separate entity. Again, given the potential variation
29 in authority and operational capacity, we propose the Attorney General in brackets.
30 Upon losing this second round, the individual may appeal to, we propose, the state
31 appellate court, which will review the second round denial for abuse of discretion.

1 **SECTION 10. MANDATORY INDEPENDENT ANNUAL AUDIT.**

2 (a) Audits Required. The [Attorney General, State Auditor, Ombudsman, or Inspector
3 General] must conduct an annual audit of the central repository and of a representative sample of
4 all repositories.

5 (b) Purpose of Audits. The annual audits must assess the integrity of each computerized
6 system and database, and each physical location storing criminal history record information, to
7 ensure this [act] is implemented.

8 (c) Nature of Audits. As part of the annual audits, the [Attorney General, State Auditor,
9 Ombudsman, or Inspector General] must:

10 (1) collect data from a representative sample of all criminal history record
11 information stored at the central repository and the audited repositories, to verify its accuracy;

12 (2) determine the number of missing reportable events and biometric identifying
13 information in the samples, in part by examining public records of the courts of [this state];

14 (3) ensure that the audited repositories are representative of the overall status of
15 the system of criminal history record information management, and that selection of repositories
16 to be audited is random and in accordance with best practices; and

17 (4) conduct an annual review of the plans, policies, and procedures of at least 5%
18 of all municipal police departments and 10% of all [judicial districts] to ensure this [act] is
19 implemented.

20 (d) Access for Audits. The [Attorney General, State Auditor, Ombudsman, or Inspector
21 General] must be given access to the government records, reports, listings, and information
22 required to conduct the annual audits. All officers and employees of the state or a political
23 subdivision of the state with relevant information must cooperate with the [Attorney General,

1 State Auditor, Ombudsman, or Inspector General], and provide information requested for the
2 annual audit.

3 (e) Public Reports of Audits. The [Attorney General, State Auditor, Ombudsman, or
4 Inspector General] must generate and make widely available a public report containing the
5 results of the annual audits and any list of deficiencies and recommendations for the correction
6 of the deficiencies.

7 *Mandatory audits.* Section 10 provides for mandatory and representative
8 audits. Audits are crucial if we are to understand how the system is actually
9 working and to prevent the automatic replication of systematic errors. If we do not
10 understand the nature and prevalence of the inaccuracies, we cannot effectively
11 address them. We again propose an entity outside of the day-to-day criminal record
12 system to conduct the audits. Here we provide a broader menu of options as several
13 potential state entities have inspection or auditing functions. The auditing process
14 will also facilitate the identification of agencies or departments failing to meet their
15 obligations under Section 5 of the act. While the central repository and other
16 parties have a menu of options to remediate these deficiencies, notably under
17 Section 11, the dissemination of the results of the audit alone should serve to
18 increase system-wide compliance, as well as to ensure the central repository is
19 fulfilling the duties set out in Section 7.

20

21 **SECTION 11. SANCTIONS AND REMEDIES.**

22 (a) Sanctions. A person that violates this [act] or implementing regulations may:

23 (1) be denied access to specified criminal history record information for a time the
24 [Attorney General] determines is appropriate.

25 (2) be subject to a civil penalty or other remedy under this [act].

26 (3) if the person is a government employee, be administratively disciplined by
27 discharge, suspension, reduction in grade, transfer, or other formal disciplinary action as the
28 employer determines is appropriate.

29 (b) Injunctions. The [Attorney General] or a subject may bring an action to enjoin the
30 central repository or a repository or a criminal justice agency or another person from violating

1 this [act] or to compel the person to comply with this [act] concerning particular pieces of
2 criminal history record information. The court may examine the criminal history record
3 information, intelligence information, or investigative information at issue in camera.

4 (c) Action for Damages. A person injured by a violation of this [act] or implementing
5 regulations has the substantive right to bring an action for compensatory damages. If the court
6 determines, by a preponderance of the evidence, that the person has been injured by a violation
7 of this [act] or implementing regulations, the court may award compensatory damages of not less
8 than \$500 for each violation, costs of litigation, and reasonable attorney’s fees.

9 (d) Criminal Penalties. An officer or employee of the central repository, a repository, or
10 a criminal justice agency who reports an event as a reportable event or intentionally discloses
11 criminal history record information with knowledge that the report or information has been
12 falsified, or who knows that criminal history record information is inaccurate and intentionally
13 fails to correct that inaccurate information with the intent to cause harm to a subject is guilty of a
14 [misdemeanor].

15 *Individual sanctions.* Section 11 provides for an array administrative, civil
16 and criminal sanctions against individuals who violate the act. It also allows both
17 subjects and the Attorney General, again in brackets, to seek injunctive relief. The
18 section affords a subject who is injured by a violation of the act a civil damages
19 remedy with a modest minimum (\$500 per violation) and a fee shifting provision on
20 the theory that the true extent of actual damages may be difficult to prove. The
21 sanctions set out in this section mirror are modeled after some existing provisions,
22 and are limited in scope. All of this, of course, is also designed to serve as a clear
23 and enforceable incentive to minimize inaccuracies.

24
25 **SECTION 12. DUTIES AND AUTHORITY OF [ATTORNEY GENERAL].**

26 (a) Duty to Adopt Regulations. The [Attorney General] must adopt implementing
27 regulations under this [act]. The regulations must include provisions that:

28 (1) govern the security, completeness, accuracy, individual access, and review of

1 criminal history record information;

2 (2) govern the conduct of audits;

3 (3) ensure that electronic data, including biometric identifying information, are
4 stored in a manner that reflects best practices for personally identifiable information; and

5 (3) set a maximum reasonable fee for the cost of disseminating criminal history
6 record information, and a policy providing free access to criminal history record information for
7 an indigent subject seeking access to the subject's own information.

8 (b) Authority to Conduct Investigations. The [Attorney General] may investigate all
9 matters relating to the administration and enforcement of this [act].

10 (c) Authority to Enforce. The [Attorney General] may bring a civil or criminal action for
11 a violation of this [act].

12 *Duties and Authorities of the Attorney General.* This administrative section
13 vests the Attorney General, in brackets, with various authorities and duties,
14 including adopting regulations and conducting investigations. As discussed above,
15 this role can be filled by another agency, as long as it has sufficient autonomy from
16 the central repository and the other enumerated parties in the act to conduct the
17 requisite checks, including the audits discussed in Section 10.

18
19 **SECTION 13. UNIFORMITY OF APPLICATION AND CONSTRUCTION.** In
20 applying and construing this uniform act, consideration must be given to the need to promote
21 uniformity of the law with respect to its subject matter among states that enact it.

22 **SECTION 14. REPEALS; CONFORMING AMENDMENTS.**

23 (a)

24 (b)

25 (c)

26 **SECTION 15. EFFECTIVE DATE.** This [act] takes effect