DOJ SUMMARY: Section 6403 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108– 458, 118 Stat. 3638, 3758–60 (2004) requires the Attorney General to report to Congress on statutorily required criminal history record checks conducted by the Department of Justice. As part of this report, the Attorney General is required to make certain recommendations to Congress for improving, standardizing, and consolidating the existing statutory authorizations, programs, and procedures for the conduct of criminal history record checks for non-criminal justice purposes, such as licensing and employment.

NBD Comment: *NBD supports the Congress' stated objective of "making fingerprint-based checks of the FBI's IAFIS more broadly available to employers." For more than two years NBD has been developing the relationships and technology needed to support innovative public-private partnerships with the state criminal history repositories and the FBI. Our objective for these public-private partnerships is to reduce the legal, cost and convenience barriers that preclude most private employers, property managers and volunteer groups from obtaining fingerprint-based and name-based criminal history checks that are national in scope.*

Professional background screening companies routinely assist employers and other end-users determine applicants' suitability to serve in the intended positions based upon criminal history information drawn from public records. However, prior to the Crime Prevention and Privacy Compact Council's (Compact Council) adoption of its "Outsourcing of Criminal Justice Functions" rule (28 CFR 906) and its companion "Security and Management Control Outsourcing Standards" (Outsourcing Rule and Standards), the professional background screening industry's resources could not be used to assist authorized employers with evaluation of CHRI returned by the FBI. This limitation bifurcated the normal applicant evaluation process that typically also includes checks of other types of data, such as credit reports, verification of educational credentials, employment and residence history and references evaluated by the professional background screening industry and the criminal history background checks of the FBI's data evaluated by a government agency or the employer.

With the acquisition of a controlling interest in PrideRock Holding Company by First Advantage earlier this year, along with our partners in Credential Services, LLC, we now have the personnel, infrastructure, technology and resources to make the public-private partnerships to complete solutions for:

1. *Facilitating efficient and convenient collection and electronic submission of applicants' fingerprints.*
2. *Channeling them to state repositories and the FBI in accordance with the Outsourcing Rule and Standards.*
3. *Drawing upon the resources of the professional background screening industry to conduct suitability evaluations of CHRI from the FBI on behalf of employers in accordance with the Outsourcing Rule and Standards.*
4. *Retaining fingerprints on behalf of applicants to resubmit them for future checks, when authorized by the applicants and biometrically confirmed that the retained prints are those of the applicants.*
5. *Auditing the companies that: (1) collect the prints, (2) order the IAFIS checks on behalf of authorized recipients and (3) receive Criminal History Record Information (CHRI) channeled from the FBI. These audits will check compliance with the applicable security and data protection requirements of the Compact Council and the Fair Credit of Reporting Act (FCRA). By having an independent, trusted third-party conduct these audits, state and federal auditors' efforts can focus on the effectiveness of the third-party's audit program in ensuring*

compliance with the applicable Compact Council, FBI and state criminal requirements regarding access, use and security of CHRI.

Because NBD is a wholesale-only provider of background screening data, we are well positioned to provide the entire professional background screening industry access to the benefits of these fingerprint-based solutions.

To make fingerprint-based checks of the FBI's IAFIS more broadly available to employers, in those cases where neither federal nor state law mandates them, will require reduction of the fees paid to the state repositories and the FBI. Eliminating requirements to conduct a state repository check in order to obtain a national check of the FBI's IAFIS would substantially reduce the cost of furnishing non-mandated checks. Requiring electronic submission of these non-mandated checks may also reduce the FBI's costs. By sharing some of the cost savings associated with electronic submission, the FBI could share some of the revenues with the state repositories to help offset the loss of their revenues associated with not first requiring a state search. To further offset the state repositories' revenue losses a combination of public-private partnerships could generate new revenues for services that the repositories are uniquely capable of providing. (See our comments on question 15.)

DOJ - In developing this report, the Attorney General must consult with representatives of state criminal history repositories, the National Crime Prevention and Privacy Compact Council, appropriate representatives of private industry, and representatives of labor. Therefore, to provide a means of input to these named parties, and to allow for broader public input on the issues that will be addressed in the report, the Department of Justice is publishing this notice seeking public comment on the development of the required report. Section 6403(d), 118 Stat. 3638, 3759 (2004). Pursuant to section 6403(d) of the Act, the Department of Justice is to consider the following fifteen factors in making the recommendations:

NBD Comment: *NBD is a compiler of criminal history databases that it uses to conduct criminal history background checks in support of the professional background screening industry, which serves a wide range of employers, property managers and other businesses. As such, it is clearly "an appropriate representative of industry." As a member of the National Association of Professional Background Screeners and the Consumer Data Industry Association it in general supports the comments of these organizations. NBD is a Service of First Advantage, a member of the First American Family of Companies.*

DOJ - (1) The effectiveness and efficiency of utilizing commercially available databases as a supplement to IAFIS [the Integrated Automated Fingerprint Identification System] criminal history information checks;

NBD Comment: *Commercially available criminal history databases developed by responsible compilers, such as NBD, provide an excellent, cost effective supplement to IAFIS criminal information checks. These databases include offenses of interest to employers that for a variety of reasons may not be returned by IAFIS. For example, some offenders' fingerprints are not captured even though they may be convicted and placed on probation and a substantial percentage of dispositions are not available in IAFIS. Furthermore, not all criminal history offense records retained by the official state repositories are returned when IAFIS checks are conducted for non-criminal justice purposes. Some of these missing offender and offense records and dispositions will be in the court records compiled in commercial criminal history databases. The nation's Professional Background Screening Companies, many of which are NBD's Affiliates, have an existing network of relationships with employers and data providers. Such a network cannot be recreated overnight.*

DOJ - (2) Any security concerns created by the existence of these commercially available databases concerning their ability to provide sensitive information that is not readily available about law enforcement or intelligence officials, including their identity, residence, and financial status;

NBD Comment - *Commercial criminal history databases do not represent a source of sensitive information about law enforcement or intelligence officials, such as their identity, residence or financial status.*

This security concern is based on other types of commercially available databases that do provide sensitive information about citizens that may otherwise not be publicly available. This is a totally separate issue, although some companies compile identity information, they do not commingle the criminal data with the identity data, even if some commercial reports might include both criminal history data and identity data.

The Outsourcing Rule and Standards includes security requirements for any CHRI provided by the FBI to channelers or professional background screeners for the purpose of conducting suitability evaluations for authorized recipients.

DOJ - (3) The effectiveness of utilizing State databases;

NBD Comment: *As indicated in (1) above, state repository databases are generally more complete than the IAFIS database. Separate fingerprint submissions to the majority of state repositories in addition to the submission to the FBI's IAFIS would be required for a non-criminal justice purposes check to be as complete as the criminal justice checks conducted thousands of times a day. We would support efforts to increase the percentage of offenders' fingerprints and offense records returned by IAFIS when it is checked for non-criminal justice purposes.*

Of course the state repositories, as well as the FBI, can only provide criminal history background checks, while professional background screening companies can provide comprehensive background checks that provide a broader view of applicants' suitability as employees or tenants. For example, these checks also include credit checks, employment verifications, driving records, reference checks and address verifications in addition to criminal history background checks.

DOJ – (4) Any feasibility studies by the Department of Justice of the resources and structure of the Federal Bureau of Investigation to establish a system to provide criminal history information;

NBD Comment - *Two of NBD's partners in Credential Services, LLC were primary contributors to the FBI's National Fingerprint-Based Applicant Check Study (N-FACS), while they were with the Ohio Bureau of Criminal Identification and Investigation. Based upon this report the FBI recommended and the Interstate Crime Prevention and Privacy Compact Council approved use of 10 flat fingerprints for identification purposes. Collection and electronic submission of flat fingerprints for civil purposes have the potential for substantially reducing the cost and increasing accessibility to fingerprint-based criminal background checks.*

A private sector consortium operated by a trusted, independent third-party, such as Credential Services, could be more cost-effective and efficient means for developing the infrastructure needed to support increased access to the IAFIS for fingerprint-based civil background checks.

NBD has publicly and privately offered to conduct screenings of the volunteers in the PROTECT Act Study for DOJ. Because we could perform these screenings using our highly efficient batch processing technology, we offered to conduct them no cost to the government as a public service in support of the PROTECT Act Study. Our results would help establish the relative effectiveness of name-based checks using commercial criminal databases versus the fingerprint-based checks

using the FBI's IAFIS. To date, we understand that contracting difficulties have prevented the FBI of taking advantage of this offer.

DOJ - (5) Privacy rights and other employee protections, including— (A) Employee consent; (B) Access to the records used if employment was denied; (C) The disposition of the fingerprint submissions after the records are searched; (D) An appeal mechanism; and (E) Penalties for misuse of the information;

NBD Comment *- The Fair Credit Reporting Act (FCRA) provides a comprehensive system for protecting employees and applicants' rights, including (A) employee consent, (B) access to records used if employment is denied, (D) reinvestigation of disputed results and (E) penalties for misuse of information, provided the employer uses the services of Consumer Reporting Agency to conduct the background check. To facilitate consistent compliance by employers, the requirements of the FCRA should be imposed on all types of background checks, whether (1) they are conducted using the services of CRAs or not, (2) whether the checks are fingerprint-based or name-based and (3) whether the checks are of federal, state or commercial criminal history databases or on-site court records. Currently, the consumers are denied the protections of the federal FCRA when employers conduct their own criminal background checks using state, federal and court resources. This inequity needs to be rectified and certainly should not be extended when expanding the types of employers who have access to the FBI's data. (Note, we do not recommend making the court system or state and federal repositories of criminal history data Consumer Reporting Agencies.)*

Currently, the FBI and many state repositories are not retaining civil fingerprints. Some state repositories are retaining civil prints and checking them in conjunction with crime scene investigations. This practice is especially disturbing when the practice is not disclosed to applicants, as we understand is the case in a few states. Some state repositories are considering retention of applicants' prints, which are checked when new offenders' prints are received to determine whether a previously cleared applicant in a sensitive position, such as a teacher, has been printed. This process is known as "rapback". While "rapback" has obvious value to employers, retention of civil prints by government agencies creates the potential that they may be used for purposes not authorized by the applicants, such as, crime scene investigations. A public-private partnership could facilitate the "rapback" process by keeping track of the various employers and volunteer organizations applicants have authorized to receive "rapback" information and reduce the potential for the applicants' prints to be used for purposes they did not specifically authorize.

DOJ - (6) The scope and means of processing background checks for private employers utilizing data maintained by the Federal Bureau of Investigation that the Attorney General should be allowed to authorize in cases where the authority for such checks is not available at the State level;

NBD Comment *- NBD supports a process by which increased access to data maintained by the FBI is available to private employers. Authorization by the Attorney General, rather than Congressional action, is a reasonable approach to providing employers who have a demonstrated public interest need for access to this data in those states that do not otherwise provide for it. For example, with the increased public and Congressional concern about protection of identity information, NBD would support providing professional background screening companies' the opportunity to request fingerprint-based criminal background checks on employees and end-user personnel that have access to large amounts of personal identity data and Criminal History Record Information from the FBI.*

DOJ - (7) Any restrictions that should be placed on the ability of an employer to charge an employee or prospective employee for the cost associated with the background check;

NBD Comment *- Currently, employees and prospective employees, such as teachers and applicants for professional licenses in many states, must pay for their fingerprint-based criminal history background checks. Most employers do not require employees and prospective employees to pay for commercial name-based background checks. For discretionary fingerprint-based criminal history background checks of the type that most employers would be conducting, NBD recommends letting the market place determine the extent to which employers are able to charge an employee or prospective employee for conducting the check.*

DOJ - (8) Which requirements should apply to the handling of incomplete records;

NBD Comment *- The FCRA requires Consumer Reporting Agencies to either: "(1) at the time such public record information is reported to the user of such consumer report, notify the consumer of the fact that public record information is being reported by the consumer reporting agency, together with the name and address of the person to whom such information is being reported; or (2) maintain strict procedures designed to insure that whenever public record information which is likely to have an adverse effect on a consumer's ability to obtain employment is reported it is complete and up to date. For purposes of this paragraph, items of public record relating to arrests, indictments, convictions, suits, tax liens, and outstanding judgments shall be considered up to date if the current public record status of the item at the time of the report is reported."*

By permitting professional background screening sompanies to conduct fingerprint-based criminal history background checks on behalf of employers in accordance with the FCRA, the burden of locating missing dispositions can be shifted from the FBI and state repositories to the CRAs. The federal FCRA limits the use of arrest records to 7 years following the arrest unless the consumer was convicted, in which case no limit is placed on the time period during which the record of the conviction can be returned. Some states place stricter restrictions on the age of conviction records that can be used, as well as use of arrest records that do not result in a conviction. Even in the states that permit use of arrest records, there is little consensus amongst employers and professional background screening companies regarding the advisability of use of arrest records that did not result in a conviction (arrest-only records) in making employment decisions. Those who argue for use of arrest only records, do so out of a concern that a series of arrests, especially involving molestation and sexual assaults, may be indicators of unacceptable underlying behavior and the lack of convictions may be more a reflection of the difficulties in obtaining convictions than the individual's innocence.

DOJ – (9) The circumstances under which the criminal history information should be disseminated to the employer;

NBD Comment *- Criminal history information from IAFIS should be returned to employers consistent with state law. Professional background screening companies should be able to assist end-users with conducting suitability evaluations of the records in accordance with the Compact Council's Outsourcing Rule and Standard. NBD's President attended the various meetings of the Compact Council and its Standards Committee during the Standard was developed, reviewed and adopted.*

DOJ - (10) The type of restrictions that should be prescribed for the handling of criminal history information by an employer;

NBD Comment *- The FCRA requires employers to maintain confidentiality of criminal history information and disposal of the results. The Compact Councils Outsourcing Rule and Standard provides additional appropriate restrictions on handling Criminal History Record Information from the FBI.*

DOJ - (11) The range of Federal and State fees that might apply to such background check requests;

NBD Comment *- Fees for conducting civil criminal history background checks have become a major, if not primary, source of funding state repositories and in some cases other essential criminal justice functions in states strapped for revenue. In recent years, background check fees have replaced reduced federal criminal justice improvement grants as the source of funds for upgrading state repositories' systems and record collection efforts. To the extent that the fees charged exceed the cost of performing the check, the fees represent a hidden tax on employers and applicants.*

Because the state repositories are so dependent upon background check fees changing the process of conducting fingerprint-based criminal history background checks for civil purposes to mirror the current process for conducing fingerprint-based checks for criminal justice purposes with a single check could destroy the very source of records. Everyone would benefit from a change in the process by which a single technical search of the FBI IAFIS would return all offender records from all states. State repositories systems could focus on their criminal justice missions, especially compiling the records, increased numbers of checks could be accommodated by increasing the FBI's infrastructure generating additional revenues that would need to be shared with the state repositories in return for their data. Security would be enhanced because the civil background checks would be more comprehensive. Privacy would be protected by increased use of fingerprint-based searches, which reduces the potential for false positives. By eliminating the need for both state repository and FBI checks, commercial name based checks can be performed to identify records of offenses for which the offenders were not fingerprinted and thus are not included in the FBI and state repositories' databases.

Increased use of flat fingerprint images for conducting civil criminal history background checks, submission of which has been approved by the FBI and the Compact Council, has the potential for reducing the cost of collecting prints.

DOJ - (12) Any requirements that should be imposed concerning the time for responding to such background check requests;

NBD Comment *- A comprehensive background check of the type conducted by professional background screening companies takes time to compile and evaluate the data. However, there still is substantial value in providing timely evaluations of applicants' suitability for employment based upon a criminal history background check. Just as in the case of the NICS gun checks, most checks can be completed very quickly. However, some applicants' records will need further review. Some mechanism is needed to ensure that employers do not discriminate against applicants just because their results cannot be returned immediately. Modern AFIS systems permit prompt turnaround of fingerprint-based background checks, provided the applicants' fingerprints are submitted electronically as soon as they are collected. For this reason, NBD's sister FADV subsidiary, PrideRock Holding Company, has developed software that allows prints to be electronically submitted as soon as they are captured, regardless of whether a livescan device is used in high volume locations or the applicant's fingerprints are captured using cards and ink in low volume locations. In that case the applicant's demographic data is collected electronically and the inked prints are verified to meet NIST standards prior to the applicant leaving the capture facility.*

DOJ - (13) Any infrastructure that may need to be developed to support the processing of such checks, including— (A) The means by which information is collected and submitted in support of the checks; and (B) The system capacity needed to process such checks at the Federal and State level;

NBD Comment *- SEARCH surveys indicate that many of the state repositories' AFIS infrastructures are having difficulty supporting the current demand for non-criminal justice background check.The demand for non-criminal justice checks may be jeopardizing vital criminal justice missions in some states. In addition, increased IAFIS infrastructure will be needed to accommodate the probable increase in fingerprint-based criminal history background checks that will occur when the Congress opens up the FBI's IAFIS to most employers. To minimize the extent to which additional infrastructure is needed, it is essential to avoid the need for multiple technical searches of AFIS databases. As indicated in our comments on question (11) eliminating the need to conduct state repository searches must not result in loss of funding the state repositories need to perform their essential criminal justice missions. The obvious solution would be for the FBI's IAFIS infrastructure to be increased to handle the load. The Next Generation IAFIS system is several years away from implementation. A less obvious solution would be for the private sector to provide a state of the art AFIS system that would contain only the offenders' prints and a unique identifier that could be used to order they offenders criminal history record when the offender's prints match those of the applicant. This private sector funded system could be funded by the Professional Background Screening Company and operated by an independent third-party in support of the entire industry. Because this system would not have the offenders' demographic data there would be little privacy concern associated with retention of the prints. If an independent third-party retains in a way that cannot be used for crime scene investigations, "rapback" can be accomplished without the privacy concerns associated with state repository retention of the applicants' fingerprints.*

DOJ - (14) The role that States should play; and

NBD Comment *- The states' most essential role is the compilation of the offenders' criminal history records and providing this information to the FBI IAFIS either as it is received or upon request. The importance of this role cannot be understated and must still be funded following the Congress' most laudable objective of increasing the efficiency and consistency of criminal history background check processes.*

NBD has been a consistent advocate of public-private partnerships in which the Professional Background Screening Industry's infrastructure is leveraged to reduce the burden on scarce criminal history repository resources, while generating revenues to support their vital compilation and criminal justice functions.

DOJ - (15) Any other factors that the Attorney General determines to be relevant to the subject of the report.

NBD Comment -

Name-based Criminal History Background Checks

We are ardent supporters of increased private sector use of fingerprint–based criminal history background checks. However, we also worked diligently to enhance the quality of name-based criminal history background checks. The majority of criminal history background checks conducted for non-criminal justice purposes are name-based checks. Name-based checks are substantially less resource intensive, less costly and for the foreseeable future available to a broader range of employers, name-based checks. For these reasons, name-based checks will continue to be the only practical option for many employers and property managers to conduct their criminal history background checks.

Employers and other end-users have access to three sources of name-based criminal history background checks:

1. ***County criminal court records*** *– Historically, criminal court records have been open for public inspection. While these records are generally the most complete, they have to be checked one court at a time, limiting the number of locations that it is practical to check. Unfortunately, based upon identity theft concerns, some court and corrections sources are increasingly limiting availability of personal identifiers, most importantly offenders' dates of birth, that increases the potential for "false positive" results that do not apply to the applicant.*
2. ***State criminal history repository databases*** *– Thirty-one state criminal history repositories offer single state name-based checks of their data. The state repositories are not able to provide name-based checks of other states' data because the Interstate Crime Prevention and Privacy Compact prohibits name-based checks of the FBI's name-based checks of the Interstate Identification Index for civil purposes. Therefore, state repository name-based checks alone are not a practical alternative for most employers, managers of multi-unit housing complexes and volunteer organizations whose applicants may have resided or worked in multiple states.*
3. ***Commercial multi-state criminal history databases*** *– include criminal history records drawn from the majority of states. They are the only affordable multi-state option available to most users whose applicants may have lived in multiple states.*

To enhance the quality of name-based criminal history background checks, NBD supports:

1. *Providing increased name-based access to the III database subject to:*
    a. *Verifying that returned offense records apply to the applicant using biometric means.*
    b. *Sharing the revenues from these checks with the state repositories as previously described.*
2. *Encouraging courts to provide bulk access to summaries of their criminal history records, including available personal identifiers to private sector compilers of criminal history databases, provided these compilers:*
    a. *Use the personal identifiers only for matching purposes.*
    b. *Implement the provisions of FCRA ¶ 613 so the records are confirmed to be current and accurate prior to release or the applicant is informed of that a record has been returned to provide the applicant an opportunity to contest the applicability or accuracy of the information.*
    c. *Promptly remove expunged and sealed records upon notification by the courts.*

Fingerprint-supported Name-based Checks

There are a variety of barriers to employers' use of fingerprint-based criminal history background checks in addition to the lack of Congressional authorization to conduct the checks. The time, cost and inconvenience associated with collecting fingerprints represents a significant barrier to use of fingerprint-based criminal history checks. As previously, mature technology is available for capturing flat fingerprints at a substantial savings in time, training and infrastructure costs, along with convenience to applicants.

While the FBI is ready to start conducting flat fingerprint-based criminal history background checks for civil purposes, most states AFIS systems need upgrades to support flat fingerprint-based criminal history background checks. Congress should provide incentives to the state repositories to encourage the early adoption of AFIS upgrades that will permit increased use of flat fingerprint capture for civil purposes.

The attached draft white paper describes a new process for conducting name-based checks, supported by capture of one or two flat fingerprints by employers. The employer submits these flat prints electronically to a trusted, independent third-party that retains the prints for use in confirming that name-based check results actually apply to the applicant. This approach provides accuracy of fingerprint-based checks in terms of assuring that offenses actually apply to the applicant. However, it uses substantially fewer scarce AFIS resources, since:

1. *Only about one in ten name-based, with a similar percentage for fingerprint-based searches, return offender records. Thus, no fingerprint comparison is required ninety percent of the time.*
2. *Only a one to one match is required to determine whether the offenders and applicant's prints match, which uses substantially fewer resources than the full technical searches that typically require comparisons with the bulk of the prints retained in an AFIS fingerprint database.*

Need for Studies of the Relevancy of Criminal History Records to Performance

We are not aware of any academic or statistical studies that have demonstrated the relevancy of various types of criminal history records to offenders' performance as employees, tenants or volunteers. We understand that Professor Alfred Blumstein of Carnegie Mellon University has conducted long term studies of criminal behavior and recidivism. However, apparently these studies have not gone beyond basic demographic parameters, such as age and years since last offense or release from supervision. Other parameters that might be important predictors of the offenders' performance as employees, tenants and volunteers, such as employment, credit, eviction, educational, and home ownership history, as well as, participation in rehabilitation, counseling and faith-based programs not been studied.

Given the importance of offenders' reintegration into society, there is strong incentive for DOJ to sponsor academic research to identify the parameters that are statistically significant. When completed the results of this research would provide a scientific basis for legislators, courts, employers, property managers and volunteer organizations' criteria regarding which offenders are good risks and which are bad risks. Private sector eviction, employment, home ownership and credit history databases would provide academicians a more complete picture of the circumstances that enabled some offenders to successfully reintegrate into society and lead others to recidivism. For example, First Advantage SafeRent has:

1. *Assigned National Incident Based Reporting System (NIBRS) based categories to the offense records in its criminal history database. Most states and none of the major cities are assigning NIBRS categories to the arrest records they submit to the FBI. Using these categories permits First Advantage SafeRent to automatically score applicants' criminal history records based upon the property managers' criteria regarding the number and types of the offenses.*
2. *The ability in most cases to accurately associate the offenders' employment, residence, eviction and credit history with their criminal history.*
3. *Developed reliable models for predicting applicants' performance as multi-family housing tenants using sophisticated econometric models and private sector databases.*

This type of information has not been available to academic researchers like Professor Blumstein and could provide the basis for the type of research into the relevancy of criminal history records we are recommending.

Encouraging Public-Private Partnerships that Leverage the Professional Background Screening Industry's Infrastructure

The Professional Background Screening Infrastructure can facilitate increased use of fingerprint-based criminal history background checks with:

a. Its criminal history databases and other data needed to complete a comprehensive check of applicants' backgrounds, such as landlord-tenant court records and credit reports.

b. Its processes for verifying applicants' references and their residence, employment and educational histories.

c. Its capability for evaluating applicants' suitability based upon the employers or property managers' risk tolerance and reasons for conducting the check.

DOJ - Congress has instructed the Department of Justice to consult with certain parties in developing the report. In accordance with section 6403(e) of the Act, the Department of Justice must consult with representatives of State criminal history record repositories, the National Crime Prevention and Privacy Compact Council, appropriate representatives of private industry, and representatives of labor, as determined appropriate by the Attorney General.

NBD Comment *- NBD is member of the National Association of Professional Background Screeners, the Consumer Data Industry Association. It has been represented on task forces convened by SEARCH and the Bureau of Justice Statistics of the Department of Justice on private sector use of criminal history records and backgrounding of America. In addition, NBD is regularly represented at meetings and symposia of SEARCH, the Interstate Crime Prevention and Privacy Compact Council and its committees, the FBI's Advisory Policy Board and Courtroom 21 Privacy of Court Records conferences. As such, NBD would seem an "appropriate representative of private industry."*

DOJ - Comments Sought The Department of Justice seeks public comment on all of the reporting requirements described in section 6403 of the Act. In particular, the Department is seeking comments responsive to the fifteen factors it must consider when making recommendations to Congress. The Department welcomes comments not just from the specific parties identified in section 6403(e) of the Act, but from any person who may be able to provide responsive information that the Department may consider when drafting the report.

NBD Comment - Comments have been provided on all fifteen factors, as well as an overview of NBD's recommendations for "making fingerprint-based checks of the FBI's IAFIS more broadly available to employers."

Biometric-Supported Name-Based Criminal History Background Checks

Robert W. Holloran, National Background Data, LLC (NBD) – *A First Advantage Company*
Michael Powers, Biometric Information Management, LLC
Alan Thomas, Credential Services, LLC

ABSTRACT

Biometric-supported name-based criminal history background checks offer a means of enhancing name-based checks with a more efficient use of government criminal history repository resources than conventional fingerprint-based criminal history background checks. An overview shows how key attributes of biometric-supported name-based criminal history background checks compare with conventional name-based and fingerprint-based criminal history background checks.

The process for conducting biometric-supported name-based criminal history background checks is described. The technical elements required for commercially viable biometric-supported name-based criminal history background checks are summarized, along with ways these elements can be used to enhance other types of background checks.

By addressing some of the concerns about name-based checks that are frequently expressed by government criminal history repository personnel, biometric-supported name-based criminal history background checks may permit increased name-based checks of both state and federal criminal history repository data in ways that would provide these repositories needed revenue with minimum impact on their personnel and infrastructure.

A trusted, independent third-party evaluator ensures that applicants' biometric information is used only for the intended background screening purpose and cannot be used by government agencies for crime scene investigations or for commercial purposes.

Criteria for Evaluating Criminal History Background Check Methods & Processes

Only two basic methods are currently in use: (1) fingerprint-based checks and (2) name-based checks. This paper introduces a new criminal history background check method that uses biometrics (a fingerprint and/or a digital photograph) to enhance the identification accuracy of name-based checks. The primary objectives of this new method are to:

1. Improve the identification accuracy of name-based checks.
2. Increase use of biometrics in private sector criminal history background checks, while avoiding the timeliness, cost, inconvenience and privacy barriers associated with traditional fingerprint-based criminal history background checks.

Improved Identification Accuracy of Name-Based Checks

A criminal history record misattributed to an applicant is called a "false positive". False positives may result when: (1) the applicant has a common name, such as, John Smith, (2) when the applicant's identity has been stolen and used when the offender was booked[1] or (3) limited date of birth information is available.[2] The Fair Credit Reporting Act (FCRA) requires Consumer Reporting Agencies (CRAs) to "follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates."[3]

NBD's professional background screening company affiliates are CRAs. To reduce the potential for "false positives" some affiliates limit name-based criminal history checks of NBD's multi-state criminal history database to "exact matches" of applicants' names and dates of births. This practice increases the potential for missing criminal history records that actually apply to the applicant, but for which there was not an exact match between the applicant's data and the offender's data maintained by the repository. For example, the order of the month and day in the date of birth may be reversed – *2/5/1965* versus *5/2/1965*, or a name might be misspelled, for example, *Halloran* instead of *Holloran*. Whether as a result of deception, or simply a clerical error, relying on exact matches would miss records that include these types of erroneous information.

Advanced matching logic is available that would return records with these types of errors. However, use of this logic increases the potential for "false positives". The availability of a reliable means of eliminating false positives permits increased use of these techniques.

Biometric-supported name-based checks can lead to fewer identification errors, both in terms of "false positives" and "false negatives."

Primary Characteristics of Biometric-Supported Name-Based Checks

Accuracy – As described above, biometric-supported name-based checks permit improved **identification accuracy** over conventional name-based checks. However, it should be recognized that fingerprint-based checks are still more successful in identifying an individual that has created a completely new identity than a name-based check of a criminal history repository's fingerprint-based database.

The **content accuracy** of the records returned by the type of biometric-supported name-based checks envisioned by this paper would be the same as for fingerprint-based checks conducted for the same purpose. In both cases the applicable state repository would be returning an identical rap sheet.

Completeness – The inherent technical advantage of fingerprint-based searches does not apply when fingerprint-based offender and offense records are not available in the fingerprint-based database that is being searched. For example, the FBI's database does not include offenders' fingerprint images that were not accepted, either because the prints did not meet its quality standards, or were associated with offenses that were below the FBI's severity threshold at the time. More importantly, the FBI's database includes only about 40% of the offense records, with the remainder available only at the applicable state criminal history repositories. Thus, a name-based check of a database that included the missing records would return records that would be missed by a fingerprint-based search of the FBI's database.

Even when a fingerprint-based check of the applicable state repository and a fingerprint-based check of the FBI's database is conducted, some offense records that are available only at other state repositories will not be returned for non-criminal justice background checks, even if there is a match with the offender's fingerprints in the FBI's database. Specifically, the offense records maintained by the states that have not ratified the Interstate Crime Prevention and Privacy Compact or signed the MOU with the Attorney General are not accessible for non-criminal justice purposes. It should be noted that all of the states' offense records are returned when either name-based or fingerprint-based checks are conducted for criminal justice purposes.

It could be argued that a name-based check conducted for criminal justice purposes would be more complete in terms of having fewer false negatives than a fingerprint-based check of a single state repository and the FBI's database conducted under the current restrictions on checks for non-criminal justice purposes. The completeness of such a biometric-supported name-based check would be further enhanced when private sector criminal history databases are checked, since they include name-based records maintained by courts for offenses for which the offenders' fingerprints were not captured and thus are not present in either the state repositories or the FBI's fingerprint-based databases.

The most complete biometric-supported name-based criminal history background check would query the databases of the FBI, the state repositories and the private sector.

Overcoming the Barriers Associated with Fingerprint-Based Checks

The type of biometric-supported name-based criminal record background checks envisioned by this paper avoids many of the practical barriers to wider use of conventional fingerprint-based checks:

1. **Timeliness** – The results of biometric-supported name-based checks are more timely, since the biometrics are captured by the employer and the vast majority of checks do not require use of the biometrics and those that do only require a one-to-one comparison.
2. **Cost** – The results of biometric-supported name-based checks are less expensive, since the employer can easily capture the required biometrics and the "no hit" checks (typically 90% when full dates of birth are available) do not require use of the one-to-one biometric comparisons.
3. **Privacy** – Biometric confirmation that the results apply to the subjects of the checks protects applicants, which is a frequently stated reason for using fingerprint-based check in lieu of name-based checks. With biometric-supported name-based checks, access to the applicant's biometrics is restricted. For example, they cannot be used in conjunction with criminal investigations. Also, employers would always receive the results from a CRA, the FCRA's restrictions on dissemination of the results[4] apply, ensuring protection of the applicants' privacy.
4. **Convenience** – Since the employer captures the required biometrics, it is not necessary for the applicant to travel to another facility to be fingerprinted. Furthermore, there is no opportunity for the fingerprints of someone other than the intended applicant to be substituted, as currently exists, when someone other than the employer captures the prints or when the person being

printed is given custody of the completed fingerprint card. The special "breeder document" controls being developed by the Compact Council's Standards Committee to ensure the correct person is being printed are not necessary when the employer captures the prints.

Conducting Biometric-Supported Name-Based Checks with a Private Criminal History Database

Two types of the applicants' biometrics are captured by employers and used, as necessary, by the Trusted, Independent Third-Party Evaluator to determine whether the "hits" apply to the applicant:

- **One or two "flat" fingerprints** are captured in a way that supports one-to-one matching with the offenders' rolled print images that are retained by repositories.
- **A digital photograph** is taken under controlled conditions that support facial recognition matching with offenders' mug shots.

Figure 1 provides a high-level flowchart of the process envisioned by this paper for conducting biometric-supported name-based checks. The process includes the following six basic phases:

1. **Employers** collect the biometrics and demographic information from the applicants, order the background screenings and submit the biometrics with a unique order number to the Trusted, Independent Third-Party Evaluator.
2. **Professional background screening companies (CRAs) and their database compilers,** such as NBD, check the accuracy of demographic information collected by the employers and conduct other types of employment background checks, such as, reference checks, employment and educational verifications (not shown), and conduct name-based searches of the database compiler's multi-state criminal history database, supplemented with on-site court checks in jurisdictions where the applicants lived that are not adequately covered by the multi-state criminal history database. If there are no "hits" during these checks, screening reports are prepared and returned to the employers with explanatory information permitting them to interpret the results and understand the inherent limitations of the searches.
3. **Database compilers** submit the Order Number and the returned offender's identifiers associated with the hits and the jurisdictions where the hits occurred to the Trusted, Independent Third-Party Evaluator for evaluation.
4. The **Trusted, Independent Third-Party Evaluator** obtains offenders' biometrics (fingerprints and/or mug shots, as available) from the government criminal history repositories holding the offenders' records for comparison with the applicant's biometrics.
5. The **Trusted, Independent Third-Party Evaluator** orders the releasable offense records associated with the hits from the government criminal history repositories that hold the records when the applicants' biometrics match the offenders' biometrics.
6. **Professional background screening companies (CRAs)** generate Consumer Reports based upon the records returned by the applicable repositories via the database compilers, provide the Consumer Reports to the employers and notify the applicants, when required by the FCRA.[5] In the event that the offenders' fingerprints and/or mug shots are not available in the jurisdiction of record's criminal history repositories, the professional background screening companies take other measures to determine whether the offenses reasonably apply to the offenders. For example, NBD is developing capability to evaluate whether anyone else with the same name and date of birth also resided in the vicinity where the offense was committed to facilitate making this determination.[6] In addition, the professional background screening companies are responsible for obtaining any missing dispositions in the offense records returned by the government criminal history repositories.

Essential Technical Elements of Biometric-Supported Name-Based Checks

Although the cost of rolled-print live scan equipment and software has become less expensive over the past several years, rolled-print live scan equipment is still too expensive, is too time consuming to use and requires too much operator training for most employers. Scanners and software for capturing flat fingerprints are less expensive, easier to use, take less time to complete the capture than rolled-live scan devices and have been approved for making submissions to the FBI.[7] However, the Ohio Bureau of Identification and the FBI are currently the only government criminal history repositories that are accepting submission of flat fingerprints for civil purposes.

The flat fingerprint-capture devices and software used by employers to conduct the biometric-supported name-based checks envisioned by this paper must have the following characteristics:

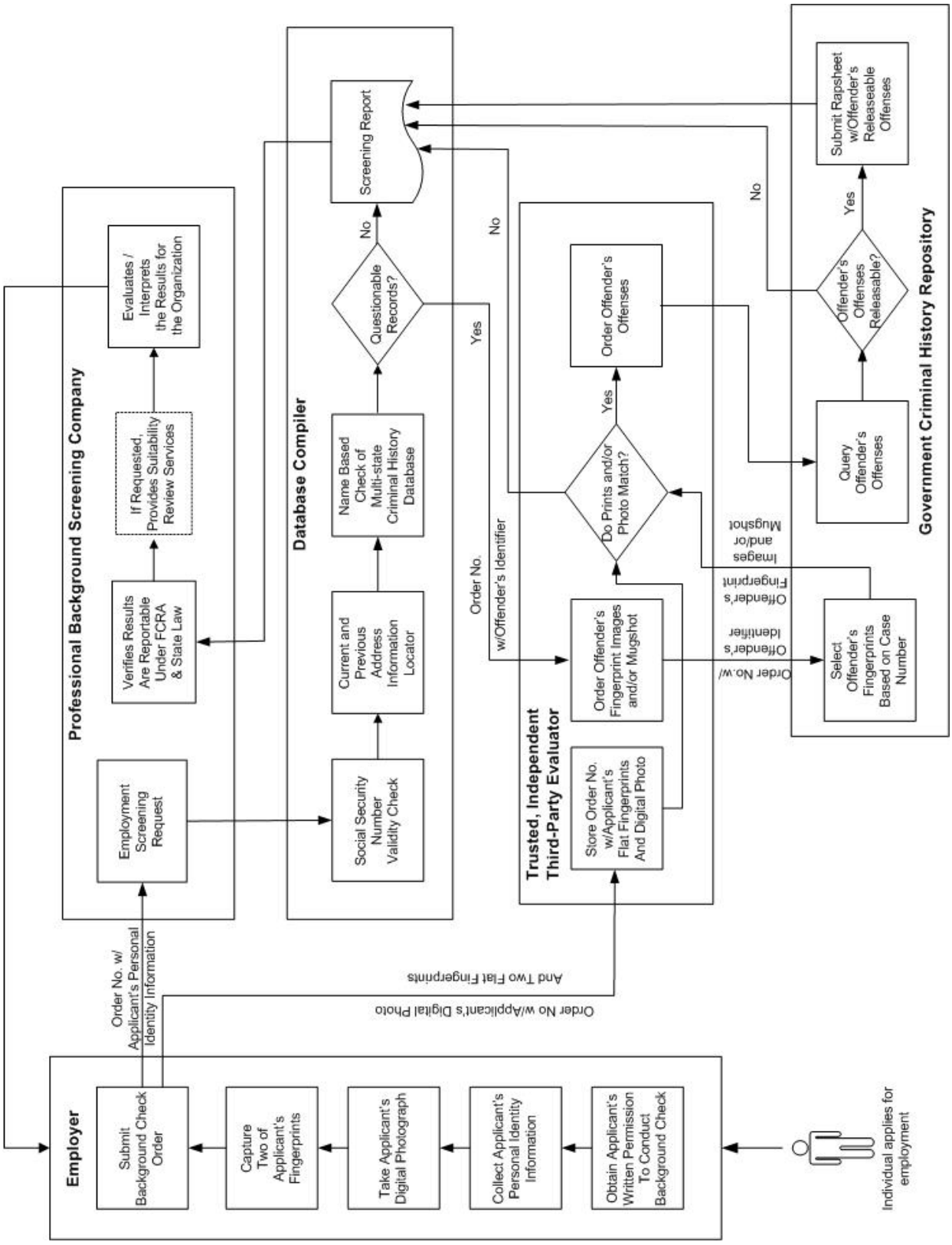

Figure 1 - Overview of Fingerprint-Supported Name-Based Criminal History Background Check Process that Relies on a Private Sector Criminal History Database

1. **Inexpensive**, ideally, the flat fingerprint capture device and the digital camera should cost the employer no more than a few hundred dollars.
2. **Easy to use**, requiring little training to capture usable flat prints in less than 15 seconds.
3. **Self-checking** to ensure that the captured prints and digital photographs are of acceptable quality. As an alternative, this quality control could take place on the Trusted, Independent Third-Party Evaluator's system, provided real-time notification appears on the employer's system if the quality is not adequate, so the defective biometrics can be recaptured while the applicant is still present.
4. **Web-based**, using SSL forms for secure transmission.
5. **Interface with existing desktop computers** used by HR departments, preferably, via a USB port.

   Interact with applicants for the purpose of informing them of their rights and to obtain their authorization to use their biometrics for the purpose of conducting biometric-supported criminal history background checks.
7. **Generate a unique order number** for each applicant's biometrics that is submitted with the biometrics to the Trusted, Independent Third-Party Evaluator and with the background check order to the professional background screening company, so any hits and demographic information submitted to the Trusted, Independent Third-Party Evaluator can be accurately matched with the applicant's biometrics.
8. **NIST compliant** submission of the flat prints and digital photographs.

The system used by the Trusted, Independent Third-Party Evaluator to determine whether offender records returned by name-based checks apply to the applicant must have the following characteristics:

1. **Accurately compares fingerprints** to determine whether the submitted flat fingerprints match the fingerprint images received from the repositories.
2. **Accurately compares facial photographs** to determine whether the submitted digital photograph matches the offender's mug shot received from the repositories.
3. **Securely protects** both the biometric data and the integrity of the process.
4. **Destroys the biometric data not used** for comparison with returned offender records.
5. **Securely retains applicants and offenders' biometric data used** to determine that the returned offender records apply to the applicants, as required by applicable laws, such as the FCRA and Sarbanes-Oxley, for use in the event the determinations of applicability are challenged by applicants, when the applicants were determined to be the offenders, or injured parties, when the applicants were determined to not be the offenders.

To minimize the potential for identity theft the Trusted, Independent Third-Party Evaluator does not receive, store or use the applicants and offenders' demographic data. The offenders' demographic information that is embedded in mug shots is not used, nor is it searchable. All of its matches are biometric based. The system generated Order Number is used to link the applicant's biometrics with the offenders' biometrics that are submitted by the repositories.

Other Uses of the Technical Elements

The inexpensive flat fingerprint-capture devices and web-based software for submitting individual flat fingerprints have other important uses:

1. Validating the intended applicant's fingerprints were used to conduct fingerprint-based background checks.[8]
2. Authorizing individuals who submit background-screening requests based upon fingerprints captured during enrollment to ensure that everyone who submits requests is authorized to do so.
3. Documenting with a biometric, individuals who submit background-screening requests for use in prosecuting criminal and civil cases against anyone who submits unauthorized requests.

Essential Characteristics of the Trusted, Independent Third-Party Evaluator

Because of the sensitive nature of individuals' biometric information, to be accepted the evaluator must be able to demonstrate that it is trustworthy to the public, the individuals whose biometric information it handles, the government agencies that provide offenders' biometric to it, the professional background screening industry and the end-users who rely on the results of its determinations. To earn this trust:

1. Its only role is to reliably determine whether applicant's biometrics match offenders' biometrics in such a way that the information entrusted to it cannot be used for any other purposes.
2. It needs to be independent of those who could use the information for other purposes.
3. It should only receive applicants' biometric data, without any personal identifiers, so there will be little potential for the data to be misused.

4. It needs strong network and physical security to ensure integrity of the process and protect the repositories and professional background screening company systems with which it connects.

Credential Services, LLC was structured to be a Trusted, Independent Third-Party Organization with a different and broader role of facilitating fingerprint-based criminal history background checks for authorized non-criminal justice purposes.[9] Many of the elements of Credential Services could be a model for the Trusted, Independent Third Party Evaluator envisioned by this paper. For example, Credential Services was structured so professionals with extensive state repository and fingerprint technology experience would audit the processes. The independence described above was achieved by assigning the LLC management role to Biometric Information Management, LLC and The Ashdale Group, Inc. personnel, even though some of its members had ties to the professional background screening industry.

Other Public-Private Partnership Benefits of Proposed Checks

NBD has been promoting public-private partnerships amongst the government criminal history repositories and the professional background screening industry for several years. Biometric-supported name-based checks was one of six potential approaches to public-private partnerships suggested in a draft paper circulated for comment at the 2004 Summer SEARCH Membership Meeting.[10] The public-private partnership implicit in the checks envisioned by this paper would provide needed revenue to the repositories, in addition to enhancing the background check processes:

1. **Capacity/Scalability** – Biometric-supported name-based checks leverage the existing professional background screening industry's extensive order processing, employer support and criminal history database infrastructure. The government criminal history repositories' AFIS capabilities are not impacted, since all requests for offender biometric and offense data will be based upon the offenders' record identifiers and will leverage existing protocols the repositories currently support for interagency transfers of biometric data and rapsheets. The Trusted, Independent Third-Party Evaluator's biometric matching infrastructure is based upon one-to-one matches, so it is not computationally intensive and is easily scalable.
2. **Security** – The person requesting a biometric-supported name-based check can be required to submit one of his/her own fingerprints, as well as two fingerprints and a digital photograph of the applicant. These submissions reduce the potential for criminal history records to be obtained without authorization.
3. **Literacy** – In addition to increased security, requiring the people who request biometric-supported name-based checks to provide one of their own fingerprints, increases accountability. The interactive interface when the biometrics are captured provides an opportunity to inform applicants of their rights with regards to the background check and its results.

Conducting Biometric-Supported Name-Based Checks Using Public and Private Criminal History Databases

Figure 2 provides a high-level flowchart of the process for conducting biometric-supported name-based checks that draw upon the offender indexes of both public and private criminal history databases. The primary difference in the processes shown on Figures 1 and 2 is the addition of a "Trusted Channeler or Compiler" that would channel name-based queries to the repositories, or conduct the name-based checks of the public and private offender indexes. The details of how these checks would be conducted have not been defined and thus are not shown on Figure 2. However, two basic approaches are possible:

1. A Trusted Channeler could act as a gateway to the existing offender indexes that reside on the repositories' servers.
2. A Trusted Compiler could compile, maintain and host a consolidated and normalized index of the offenders in the public and private criminal history database. This approach would permit consistent use of advanced matching logic to increase the probability of locating all of the applicants' offender records.

Of course, a combination of these two approaches is also possible. In any case the public and private data providers would be compensated for the data they provide, using a to-be-determined equitable formula. All of the private sector entities that transmit or receive criminal history information, including the Trusted Channeler or Compiler, would be subject to the Compact Council's "Outsourcing Rule"[11] and its companion standard.

Essential Characteristics of a Trusted Channeler or Compiler

Currently, there are many organizations; public and private, involved with background screening, which are

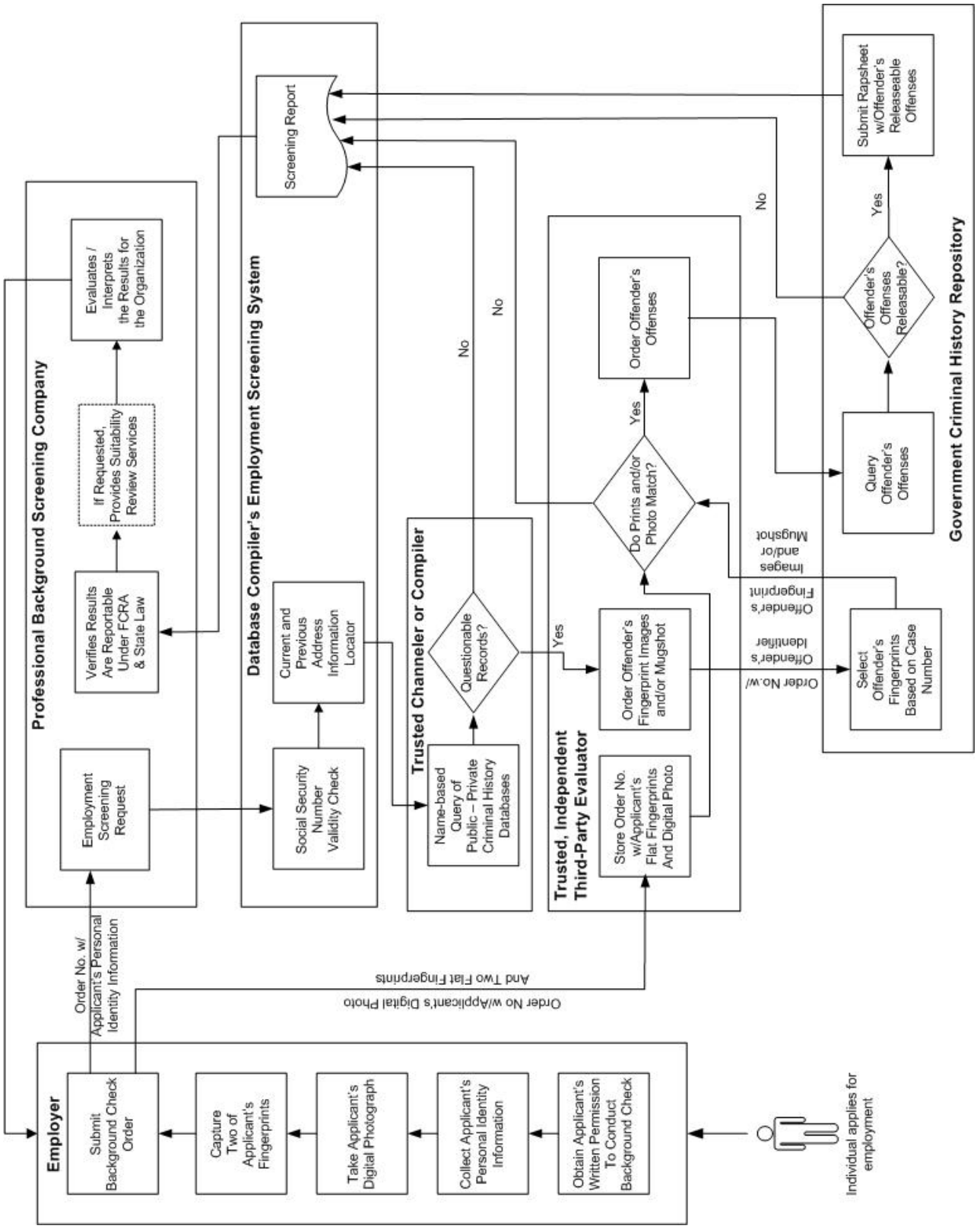

Figure 2 - Overview of Fingerprint-Supported Name-Based Criminal History Background Check Process that Queries Multiple Public-Private Sector Criminal History Databases

channelers of background screening orders and results. Some of these are also compilers of criminal history databases, like NBD. The FTC regulates the professional background screening companies as Consumer Reporting Agencies under the FCRA.[12] They are restricted from using the applicants' information for any other purposes. Although many jurisdictions have provided bulk criminal history data with the offenders' dates of birth without any restrictions on its use, responsible criminal history database compilers use of the offenders' dates of birth only for matching purposes. They do not "publish the offenders' personal identity information on the Internet" so anyone can look up offenders' personal identifiers. To be a Trusted Channeler or Compiler:

1. Its only role is to reliably determine whether applicant's demographics match offenders' demographics in such a way that the information entrusted to it cannot be used for any other purposes.

2. It needs to be independent of those who could use the information for other purposes. **3.** It should only receive applicants' personal identifiers, without any biometrics, limiting the extent to which the personal identifiers might be misused.

4. It needs strong network and physical security to ensure integrity of the process and protect the repositories and professional background screening company systems with which it connects.

5. It needs to have the infrastructure and credibility necessary to support the entire the professional background screening industry to limit the impact on technical and administrative infrastructures of the public criminal history repositories.

FBI Two-Print Pilot with the Department of State (DOS)

An FBI/DOS pilot demonstrates some of the essential elements of biometric-supported name-based criminal history background checks envisioned by this paper.

- **Fingerprints are being used to resolve uncertainties in name-based checks**, as described in an FBI Staff Paper. "The DOS conducts name checks of visa applicants at Embassies and Consulates through the Consular Lookout and Support System (CLASS). CLASS is a non-biometric based database maintained by the DOS. When the visa applicant's name hits against NCIC and/or III data in CLASS, the DOS may decide not to issue the visa based on that information. When a consulate or embassy cannot make a determination based on the name hit in CLASS, the Consulate or Embassy mails ten-rolled fingerprints to the National Visa Center (NVC). The NVC scans the fingerprints and submits them electronically to the CJIS Division."[13]

Biometric-supported name-based checks are intended to be an enhanced alternative to conventional name-based checks, not as a replacement for fingerprint-based checks that are required by existing state or federal law.

- **The FBI is using two flat prints of applicants to verify on a one-to-one basis that they match those of a previously identified offender**. The same FBI staff paper summarizes this process. "… the two-print pilot is initiated when the visa applicant applies for a visa at the Consulate and submits their biographical information along with two fingerprint images, the right and left index fingers. (These are the same two fingerprints that are used for the Biometric Visa Program.) The two prints are searched against the Department of Homeland Security's (DHS) United States Visitor and Immigrant Status Indicator Technology System's (US-VISIT) watch list, known as the Automated Biometric Identification System or IDENT. If the US-VISIT search returns no matches to the IDENT watch list, no further fingerprint processing occurs. If the applicant's two-prints are identified with a record contained in IDENT, the US-VISIT system returns an indication of the hit and the FBI number. At this point, the Consulate's office submits the applicant's two prints with the referenced FBI number, electronically to the CJIS Division. The CJIS Division performs a fingerprint image comparison to verify that the two prints match the fingerprint images associated with the referenced FBI number. Once the identification is verified, the CJIS Division responds directly to the Consulate with the CHRI."[14]

CONCLUSION

Biometric-supported name-based checks have the potential to expand the use of biometrics in private sector background checks. These checks provide enhancements over conventional name-based checks, while overcoming many of the barriers to expanded use of conventional fingerprint-based checks. The primary privacy protection reason for conducting fingerprint-based checks is retained, justifying inclusion of FBI

name-based data in the name-checks. Use of fingerprint-supported name-based checks will help mitigate the increased reluctance by courts, and other sources of public records containing criminal history information, to provide personal identifiers.

---

[1] *No Place to Hide*, Robert O'Harrow, Jr., Free Press, 2005, p80-83, 86-91, 95-97, describes the ordeal of Michael Berry when a criminal stole his identity, used Berry's identity when booked and subsequently committed murder.
[2] Increasingly, courts and other sources of public records are redacting personal identifiers from the bulk data provided to criminal history database compliers. If only the offender's birth year is provided, offenders with 364 other dates of birth would be falsely returned.
[3] 15 U.S.C. § 1681. § 607.
http://www.ftc.gov/os/statutes/050131fcra.pdf
[4] FCRA § 615.
[5] FCRA § 613 & § 615.
[6] *Public – Private Partnerships, A Way to Make Background Checks of Volunteers More Effective and Efficient?*, Robert W. Holloran, 7/20/04, p. 3. Draft circulated at SEARCH Membership Meeting. Copies available from the authors upon request.
[7] National Fingerprint-Based Applicant Check Study (N-FACS), CJIS Division, FBI, 4/5/2004.
[8] *The Credential Services Total Solution*, R. W. Holloran, M. Powers, A. Thomas., Rev 1, 12/6/2004, p. 3. Copies available from the authors upon request.
[9] Op. cit., Holloran, M. Powers, A. Thomas.
[10]Holloran, *Public – Private Partnership,* op. cit., pp 3-7.
[11] 28 CFR 906.
[12] FCRA § 603 (f).
[13] FBI Staff Paper presented at the National Crime Prevention and Privacy Compact Council Meeting on May 11, p 2.
[14] Ibid., p 2-3.