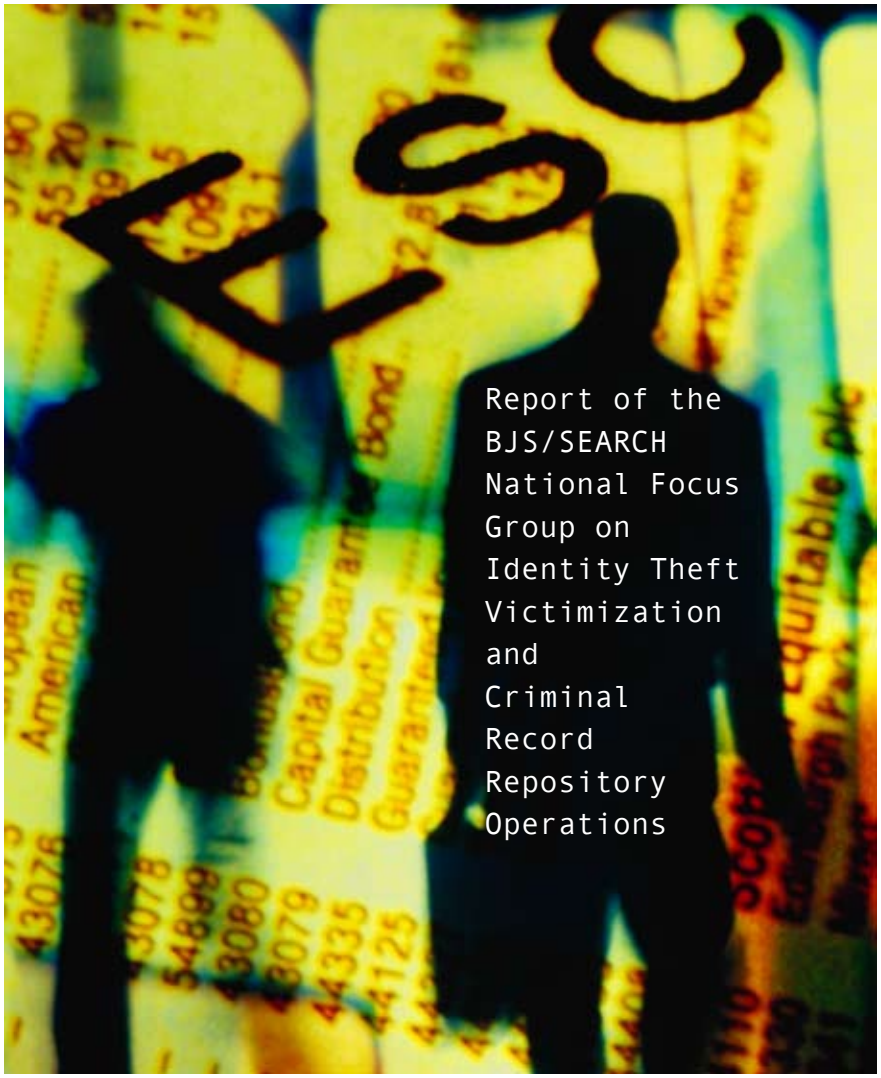


CONTENTS

Report of the BJS/SEARCH National Focus Group on Identity Theft Victimization and Criminal Record Repository Operations

The Focus Group on Identity Theft Victimization and Criminal Record Repository Operations was convened under the auspices of the Bureau of Justice Statistics (BJS), U.S. Department of Justice, and SEARCH, The National Consortium for Justice Information and Statistics.

The focus group was convened in recognition of the fact that the burgeoning national problem of identity theft, as it affects criminal history records, creates a conflict for State criminal history record repository officials as they try to balance the concerns and interests of identity theft victims with the need to maintain and disseminate records that accurately reflect arrest information as recorded at the time of booking.

Given the well understood incidence of use of false identities by arrested persons, identity issues are hardly new to the criminal justice system and certainly not for the State criminal records repositories. However, policymakers, the FBI, and State criminal records repository administrators increasingly recognize that identity theft victimization cannot be satisfactorily addressed by simply characterizing a name as an alias or "also known as." Members of the group included, in addition to BJS and SEARCH personnel, several State repository directors, FBI officials, city legal services attorneys, a court official, a university professor, and other individuals who have done extensive research and have acquired considerable expertise in issues related to the maintenance and use of criminal history records.

The focus group met on March 15, 2005, in Columbus, Ohio. Focus group participants are listed on page 10. This report summarizes the focus group's discussions and sets out its conclusions and recommendations.

Scope of Focus Group Discussions

A September 2003 report on identity theft prepared for the Federal Trade Commission (FTC) estimated that almost 10 million Americans had discovered that they were victims of some form of identity theft in the previous year.[1] The great majority of respondents to the report's underlying survey (85%) reported that their personal information was used in some sort of financial fraud, such as opening credit card accounts, taking out loans, renting apartments, or obtaining medical care or other services.

The remaining 15% of respondents reported that their personal information was fraudulently used in nonfinancial ways. The most common such use was for someone to present the victim's name and other identifying information when stopped by law enforcement authorities or when arrested or charged with a crime. Four percent of survey respondents who were identity theft victims reported that their information was misused in this manner. This suggests that almost 400,000 Americans were victimized in this way in the year prior to the survey.

[1] *Federal Trade Commission – Identity Theft Survey Report,* prepared by Synovate, September 2003. Available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

Focus group members noted that victimizations resulting from this kind of identity fraud fall into two main categories:

1. First, victims may be stopped, detained, or even arrested and charged by law enforcement officials on the basis of other persons' criminal history records.

2. Second, victims may be denied employment, licenses, housing, loans, or other services or entitlements because criminal history checks indicate that they have criminal records when, in fact, those records belong to other persons who have intentionally impersonated the victims when arrested or who have used names and other identifying information that are identical to or similar to the victim's name and identifying information.

The focus group directed its attention to these types of nonfinancial identity thefts or identity mistakes, because both are directly affected by criminal history record repository procedures and criminal history record search procedures, for both criminal justice purposes and noncriminal justice purposes.

Focus group members described personal histories of persons known to them who have repeatedly been stopped by law enforcement authorities or even taken into custody on warrants because their names and other identifying information have been intentionally or unintentionally used by other persons who have been arrested or convicted of crimes. Other members reported on personal histories of individuals who have been repeatedly denied employment, housing, or other entitlements because criminal history checks have indicated that they have criminal records when, in fact, they do not.

Types of Identity Theft and Identity Mistakes

Criminal record identity mistakes of the kind that concern the focus group result from both intentional identity theft and accidental identity mistakes. The focus group identified **three distinct situations** that can result in victimization.

Intentional Identity Theft

Arrested persons may intentionally use the names and identifiers of relatives or acquaintances whom they know to have no criminal records in order to avoid discovery of their own past records which, if discovered, would preclude their release on bail or otherwise disadvantage them.

This is a form of true identity theft that can result in severe and continuing victimization for the person whose identity is appropriated.

Legal services attorneys on the focus group presented case histories of several individuals who have been victimized in this way. In one case, a female certified nursing assistant who has no criminal record has been denied employment opportunities over a 20-year period because her identity was stolen by an acquaintance who used her name and identifiers on numerous occasions when she was arrested. In another case, an individual has been denied employment and has had encounters with law enforcement officials because his name and identifiers were used as an alias by his brother when he was arrested. In both cases, the individuals have been unable to persuade criminal record repository officials to delete the stolen identity information.

Inadvertent Identity Theft

In other cases, an arrested person may use a made-up alias without knowing that the identity belongs to or closely resembles another person who will be victimized by the impersonation. Legal aid attorneys presented a case history of an individual who has lost a job opportunity and believes he may have lost other opportunities because a person unknown to him who has an extensive criminal record used his name as an alias when he was arrested. In this case, too, State repository officials have refused to expunge the alias information.

Nontheft Identity Mistakes

In still other cases, an arrested person may use his or her true name and identifiers, which turn out to be identical or closely similar to those of another person who is later victimized by mistaken association with the arrested person's criminal record.

State repository officials conceded that this type of identity mistake with victimization consequences is a problem that has been around for a long time, since decades before identity theft was identified as a national problem. Criminal history search mistakes of this kind are generally referred to as "false positives."

Effect of Better Booking Practices

Some focus group members suggested that law enforcement officials might be able to help reduce the number of intentional false identity problems by taking more care to determine the true identities of arrested persons during the booking process, such as by asking for driver's licenses or other picture identification documents. It was pointed out by other members, however, that it is practically impossible to determine the true identity of a person who wishes to hide it.

Some criminals carry no identification in order to make it easier to use aliases. In addition, high-quality false identity documents are easy to obtain on the street and by means of the Internet. Even when the booking process includes an immediate fingerprint-based criminal history check by means of live scan fingerprint capture and automated fingerprint search equipment, identity impersonations cannot be entirely prevented. A fingerprint-based criminal history check may show that a person has a criminal record under a different name from the one given at booking, or has multiple arrests under several other names (which are consolidated by means of fingerprint identification), but there is no practical way to be sure that any of the names is the person's true identity.

Effect of Fingerprinting

Most criminal record identity thefts and mistakes can be discovered (even though victimization consequences of the kind described earlier cannot always be prevented) by using fingerprint searches instead of

searches based on names and other nonunique identifiers.[2] Recent studies and analyses have confirmed that name searches without backup fingerprint searches are unreliable. In particular, a study conducted in 1998—which evaluated the use of name searches of the Interstate Identification Index system as part of FBI criminal record screening of employment and licensing applicants—confirmed that solely name-based searches result in significant numbers of both false negative and false positive identifications.[3] As noted earlier, false positives are of particular relevance to the issue of identity theft and identity mistakes of the kind discussed by the focus group. The 1998 analysis confirmed that 4.9% of the applicants in the study were identified by initial name searches as having criminal history records, but follow-up fingerprint searches proved that these persons did not have records. If follow-up fingerprint searches had not been performed, these applicants might have unfairly been denied jobs or licenses or other benefits or entitlements.

[2] Some types of criminal justice information that may be the basis for a law enforcement encounter are not fingerprint-based, including arrest warrants and investigative information.

[3] *Interstate Identification Index Name Check Efficacy: Report of the National Task Force to the Attorney General,* July 1999, available from the Bureau of Justice Statistics, U.S. Department of Justice or at http://www.search.org/files/pdf/III_Name_Check.pdf.

Similarly, a review and analysis conducted by the FBI of fiscal year 1997 transactions involving 6.9 million civil fingerprint submissions found that 8.7% were matched with criminal records, while 33.7 million National Crime Information Center (NCIC) name check inquiries yielded "an astonishing 39.34%" hit rate. Given the concern that many of the name inquiries were related to criminal investigations, the analysis was culled down to focus on just those name inquiries (6 million) conducted for national security checks under the Security Clearance Information Act[4] and for criminal justice employment. Even with this more select population, some 16.2% of the names checked resulted in "hits." When contrasted with the 8.7% of civil applicants who are historically identified by fingerprints as having criminal records, the FBI concluded that at least 7.5% of the name search hits were false positives. "Because of the confidentiality typically associated with personnel decisions and criminal history record information, an applicant incorrectly identified may well not have an opportunity to challenge the incorrect determination and denial of employment or volunteer opportunities."[5]

However, in noncriminal justice settings, such as employment screening, fingerprint checks are expensive at both the State and Federal levels and are sometimes slow, taking weeks or even months for results to be returned. As a result, the majority of such checks, where permitted, are conducted by name searches, particularly at the State level. Indeed, State and local criminal justice agencies, such as courts, corrections agencies, and even the State criminal record repositories, are increasingly making their criminal history databases available on-line on Web sites that can be accessed by name searches. Additionally, private organizations annually conduct millions of criminal record background checks for employment purposes and other non-criminal justice purposes, based on name checks.

State Legal and Administrative Efforts to Help Victims

Some States have enacted laws or established administrative procedures to help deal with the types of identity theft or identity mistakes discussed in this report.[6] Some of these laws make it a crime for anyone to knowingly and intentionally provide a false name, social security number, or other identification information to a law enforcement officer or criminal justice official following an arrest or other criminal justice system encounter.

Several States provide a procedure for a person whose name or other identifying information has been mistakenly associated with an arrest, summons, complaint, indictment, or conviction to petition a court for a finding of factual innocence. If the court makes such a finding, it may (or in some cases must) order the petitioner's name and associated identifying information to be sealed or expunged from court and law enforcement records or be labeled to show that the information is inaccurate or has been associated with an identity mistake.

[4] 5 U.S.C. §9101.

[5] Taken from testimony of David R. Loesch, Assistant Director in Charge, Criminal Justice Information Services Division, FBI Testimony before the House Committee on the Judiciary Subcommittee on Crime, May 18, 2000.

[6] States that have enacted laws (or have bills pending) to deal with some aspects of identity thefts of the kind discussed in this report include Colorado, Illinois, Iowa, Massachusetts, Mississippi, Missouri, Montana, Nebraska, New Mexico, Ohio, Oklahoma, and Virginia.

Several States have by law or administrative procedure provided a process for persons who are the victims of identity theft or identity mistakes to obtain an "Identity Theft Passport" in the form of a card or certificate stating that the person is factually innocent of a crime or has been the victim of an identity theft or identity mistake. These passports commonly are issued by the State attorney general after a court finding of factual innocence or in some cases after the filing of a police report alleging identity theft.

Focus group discussions suggested that such laws and procedures are helpful, but not fully effective. Some members noted that the procedures for obtaining judicial determinations of factual innocence and identity theft passports are in some cases burdensome to the point that victims may be deterred from petitioning or applying. In addition, while identity theft passports may help victims avoid being mistakenly detained or arrested by law enforcement officials, they do not preclude victims from repeatedly being stopped by law enforcement officers on the basis of mistaken identities.

In the noncriminal justice setting, identity theft passports are even less effective, because a job or housing applicant, for example, may not know that a criminal record search will be conducted and, if the application is rejected, the person may not know the basis for the rejection. It was suggested that persons who have obtained identity theft passports might follow the practice of submitting a copy of the document when applying for employment, housing, and the like. However, some focus group members stated that their experience suggests that such a practice might be counterproductive because it might arouse an employer's suspicions and cause the application to be rejected on the basis of the passport alone. In addition, there have been documented cases in which employment applicants and other types of applicants have been rejected repeatedly over long periods of time and, thus, without ever having obtained an identity theft passport or pursued other remedies.

Expunging and Sealing Identity Theft-related Criminal History Information

Some focus group members felt that the most effective remedy from the standpoint of the identity theft victim was for the fraudulent or mistaken identification information to be expunged from criminal history records maintained by the State repositories and other criminal justice agencies. Other members pointed out that expunction is not appropriate in many cases, because even intentionally-assumed aliases are valuable pieces of criminal record information for law enforcement purposes.

A record subject who has used an alias may later use it again, and if the earlier alias has been expunged, the record may be missed in a search. Further, if the record subject learns that the alias has been deleted, he or she will be able to use it again with impunity. In addition, if the false name is the only name on the record, either because the criminal offender has been arrested only once or has used the same alias for multiple arrests, expunction of the name will mean that the record will be unsearchable. Finally, as noted earlier, names that cause criminal history record identity

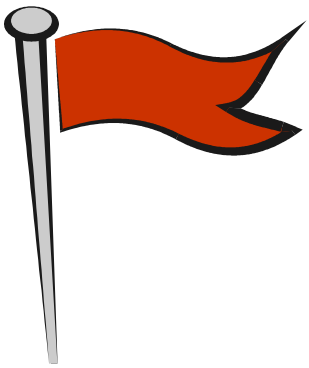
mistakes are not always false names. They may be the true names of the record subjects and identity mix-up problems of the kind under discussion may occur because other persons have the same or closely similar names and other identifiers. In such cases, expunction seems to be an inappropriate remedy from the standpoint of law enforcement effectiveness.

A less drastic remedy than expunction is sealing. Although the two terms are not used with consistent meanings in State and Federal laws, *expunction* most commonly refers to the destruction of information while *sealing* usually means that the information is retained in information systems but its availability is restricted.

In the criminal history record arena, sealed information usually is available to criminal justice officials for criminal justice purposes or for certain such purposes, such as sentencing, but is not available for noncriminal justice purposes such as employment screening, except in limited circumstances involving national security or vulnerable population groups such as children or elderly persons.

Several focus group members felt that sealing might be an effective remedy in identity theft cases, or at least a more appropriate remedy than expunction. Under this approach, names on criminal history records that have been involved in confirmed cases of identity theft or other forms of mistaken identity would be accessible for criminal justice purposes, but would not be accessible for noncriminal justice searches.

Flagging Records Associated with Identity Theft Victimization



A final remedy discussed by the focus group entails the labeling or flagging of names and associated identification information that have resulted from identity theft or have been the basis for mistaken identifications.

Under this approach, the information would remain available and searchable, but would be flagged or labeled to indicate that the information is fraudulent and does not reflect the true identity of the record subject or that it has been the basis of a mistaken identity. Such flags might also include the suggestion or direction that appropriate measures be used by record recipients to further avoid such identity mistakes, including the obtaining and submission of fingerprints.

However, some focus group members felt that, while this approach might be helpful, it would not be fully effective, particularly in noncriminal justice settings, because employers and other record recipients might not heed the warning and take the cautionary steps suggested or might simply be suspicious and reject the application to be safe. It was suggested that States might enact laws requiring employers and other record recipients to obtain fingerprints to confirm the identification if the record is flagged, or to provide to the applicant a copy of any criminal history record obtained as part of application processing, whether or not the record is the basis for a rejection. Again, the reaction of some focus group members was that such laws might be helpful, but not fully effective, because they would be difficult to enforce.

Federal Identity Theft Databases

Focus group members discussed two national-level automated identity theft databases that can be helpful to victims and to law enforcement officials.

Federal Trade Commission Identity Theft Clearinghouse

The FTC maintains an online identity theft clearinghouse that includes complaints filed by victims and complainants of identity thefts of all kinds, financial and nonfinancial. The site provides an online ID Theft Complaint Form that victims can use to file complaints.[7] These complaints are stored in Consumer Sentinel, a secure database available to law enforcement officials and investigators worldwide.[8] Complaints are also received from other sources, including some law enforcement agencies.

Federal Bureau of Investigation Identity Theft File

The FBI activated an identity theft file in April 2005, as part of its Criminal Justice Information Services (CJIS) Division-administered National Crime Information Center. The NCIC Identity Theft File provides law enforcement officials with a means to flag stolen identities to help identify imposters and assist victims. When an identity theft victim reports the incident to a law enforcement officer, the officer collects information from the individual to create a victim profile that can be entered into the Identity Theft File. The profile includes the victim's name, date of birth, social security number, and other identification information, as well as the type of identity theft. Photographs can also be entered. The officer also enters a password selected by the victim. If the victim subsequently experiences any police encounters, the police can verify the password by means of an NCIC check and can avoid any inappropriate detention or arrest.[9]

Conclusions and Recommendations

On the basis of its discussions, the focus group concluded that, although identity theft and related identity mistakes undoubtedly victimize a great number of people, the group was not prepared to recommend specific procedures and remedies to be employed by the State repositories and other criminal justice agencies to deal with the problem. It felt that not enough is known about some aspects of the problem, particularly the extent to which some of the suggested solutions might adversely affect the effectiveness of law enforcement.

For example, although expunction of stolen identification information from criminal history records would be perhaps the most effective remedy from the standpoint of identity theft victims, such an approach would hinder law enforcement effectiveness to an extent not currently quantifiable. Sealing or flagging of the information would be a more palatable remedy for State repository officials and other law enforcement officials, but might not be as effective in preventing repeated victimizations. Identity theft passports and passwords apparently are effective in preventing inappropriate detentions and arrests following law enforcement stops of identity theft victims, but are of less use in preventing victimizations in connection with applications for employment, housing, and the like.

For these reasons, the focus group felt that more information gathering and analysis needs to be done before clear-cut guidelines for State repositories can be formulated or model laws can be developed. There was general agreement within the group that a state-by-state survey or analysis

[7] http://www.consumer.gov/idtheft/

[8] http://www.consumer.gov/sentinel/index.html

[9] Information provided by Buffy Bonafield, Identity Theft File Manager, FBI, 1000 Custer Hollow Road, Module C-3, Clarksburg, WV 26306, **bbonafie@leo.gov**.

would be a useful way to collect some of the needed additional information. Issues to address in such a survey or analysis include:

1. What procedures do law enforcement agencies employ at booking to try to establish the true identities of arrested persons? Are there better procedures that might help prevent the use of aliases?

2. What procedures and remedies are in effect in law enforcement agencies and the State repositories to help prevent identity theft victimization and to help victims deal with the ensuing problems? How have these remedies worked?

3. To what extent is law enforcement effectiveness adversely affected by the expunction from criminal history records of stolen identity information when it is detected? Are there adverse effects of sealing or flagging?

4. What is being done and what more can be done to educate the public, including actual and potential identity theft victims and employers and other record recipients, about the extent of the problem and available remedies?

5. How do the name check procedures that are in effect in the State repositories actually work and are there improvements that can be incorporated to reduce the likelihood of identity mistakes? Are name check procedures used by criminal justice personnel different from those in effect when private individuals have online access to do name searches of public databases or when commercial vendors conduct name searches of their databases?

6. Do any of the State repositories or other agencies maintain identity theft databases of the kind maintained by the FBI and the FTC? How are such databases structured and who has access to them and for what purposes?

7. Can the record-review and correction procedures in effect at the Federal level and in all of the States be used to help alleviate the problems of identity theft and identity mistakes?

BJS/SEARCH National Focus Group on
Identity Theft Victimization and Criminal Record Repository Operations

Members

Mariam Aukerman
Western Michigan Legal Services

Buffy Bonafield
Federal Bureau of Investigation

Dr. Kelly Buck
Department of Defense Personnel Security Research Center

Sharon M. Dietrich
Community Legal Services, Philadelphia, Pennsylvania

Steven C. Hollon
Supreme Court of Ohio

Barry LaCroix
Massachusetts Criminal History Systems Board

Mike Lesko
Texas Department of Public Safety

Prof. Kent Markus
Capital University Law School, Ohio

John E. Monce Jr.
Ohio Bureau of Criminal Identification & Investigation

Liane M. Moriyama
Hawaii Criminal Justice Data Center

Donna M. Uzzell
Florida Department of Law Enforcement

Bureau of Justice Statistics

Gerard F. Ramker, Ph.D.

SEARCH

Owen Greenspan
Law and Policy Director

Paul Woodard
Senior Counsel

Eric Johnson
Justice Information Services Specialist

Report of work prepared under Cooperative Agreement Number 2000-MU-MU-K006, awarded to SEARCH Group, Incorporated.