

November 26, 2002

“National” Criminal History Databases

Issues and Opportunities in Pre-employment Screening

By Carl R. Ernst and Les Rosen

1. Introduction

A basic component of the background screening process with respect to an applicant for employment is a search of court and other records maintained by government agencies for the purpose of determining whether the applicant has any criminal history that is germane to the position the applicant seeks. This component is usually called a **criminal history investigation**. Since the passage of the **Fair Credit Reporting Act (FCRA)**¹ in 1970, this kind of background screening has been subject to legal constraints² whenever an employer utilizes an outside agency—usually known as a **pre-employment screening firm**—to perform the screening. Under the FCRA, these screening firms are defined as **consumer reporting agencies (CRA’s)**, and their reports are defined as **consumer reports**. The end users of these reports are **employer clients** of CRA’s. Since the subject of this article is focused on criminal history investigations by pre-employment screening firms, we will use the acronym “CRA” as shorthand for “a pre-employment screening firm that is conducting a criminal history investigation” throughout this article.

Sources of Criminal History Information

There is some confusion about what criminal history information includes. There are only three original sources of such information:

- (1) **Court records**—local, state or federal—contain incidents of arraignment, trial and disposition of cases.
- (2) **Law enforcement agency records** contain incidents of complaint, investigation, arrest, and indictment.
- (3) **Corrections agency records** contain information about probation, parole and incarceration.

Availability of Criminal History Information

Courts traditionally make their underlying paper case documentation available to the public at the courthouse, and make case summary or index information available both on-site and through remote connections, such as the Internet. Law enforcement agencies also allow on-site access to documentation such as arrest blotters, but traditionally do not themselves maintain indexes to the documentation. Corrections agencies also make their information and indexes available in a variety of ways.

¹ In this article we will refer to sections of the Fair Credit Reporting Act in the following fashion: “FCRA 613(a)(1)” is section 613(a)(1) of the act.

² In addition, the federal EEOC and state laws related to FRCA and EEOC place further limitations on using information about applicants garnered from background checks or other sources. Discussion of these laws is beyond the scope of this article.

State and local courts, law enforcement and corrections agencies in each state provide case summary and indexing information to a **statewide central repository**, which maintains and updates a computerized database of the information it receives.³

Private vendors are able to purchase some of this criminal history information from some of these agencies in some of the states, as well as from federal sources, in order to offer proprietary databases of criminal history information on CD-ROM or through web access.

Traditional Criminal History Searches

Until recently the conduct of a criminal history investigation involved one or more of the following steps:⁴

- (1) Conduct a search on the applicant's name in state and local courts located in the counties where the applicant has lived or worked.
- (2) Conduct a search on the applicant's name in federal courts in districts where the applicant has lived or worked.
- (3) Request a search from the agency that maintains the statewide criminal history databases, where available, for states where the applicant has lived or worked.

Many investigative and local public record retrieval firms offer these types of criminal record searches in the more than 3,600 counties, 10,000 federal, state and local courts and 50 state central repositories around the US. BRB Publications, Inc. (www.brbpub.com) publishes national directories listing these kinds of firms and summarizing information about the government agencies from which criminal history information can be obtained.

These public record retrieval firms may conduct FCRA-compliant criminal record searches in a number of ways:

- (1) They go in person to the courts and other government office. At the courts, they either utilize a public-access court computer or filing system, or a government clerk performs the actual search based on a requested subject name.
- (2) They phone or mail the request to the office.
- (3) They remotely access the official online database of the office.

Uses of Criminal History Information

Criminal history information is usually considered to be available to the public, with some restrictions:

- (1) Court records are generally open to the public unless the records have been sealed.
- (2) Local law enforcement agency records are generally open to the public, but statewide criminal history repositories restrict access in various ways.
- (3) Corrections agency records are generally available to the public.

³ However, federal court, law enforcement and corrections agency information is not reported to these statewide repositories.

⁴ More extensive procedures, such as checking incarceration records or even statutory access to the non-public NCIC file, are utilized if the employment position is sensitive or high level, or mandated by a governmental agency, such as fingerprint checks for teachers.

Any criminal history information that is reported to an employer is considered to be a “matter of public record” under the FCRA (FCRA 613(a)).

Criminal history information, as well as other types of information from government agencies, may be used for purposes that have nothing to do with the FCRA. For example, it may be used to check whether a potential business partner has a criminal history or to locate a deadbeat. This article focuses on the use of criminal history information in employment decision-making.

A determination of whether criminal history information is subject to the FCRA depends on whether the information is part of a consumer report, according to the following rules.

- (1) Public record information in the hands of the government agency that disseminates it is not a consumer report.
- (2) Public record information obtained directly from a government agency by an employer is not a consumer report. An employer who obtains public records directly from government agencies is not subject to the FCRA, even if the information is adverse to, and used to deny employment to, an applicant.
- (3) Public record information obtained by a CRA (from a government or a proprietary database, for example) as a mechanism to obtain leads about where to conduct searches of actual court records is not a consumer report since nothing is reported. This is commonly, but incorrectly, called “verification” in the pre-employment screening industry. If, however, this raw lead data is reported to an employer client, it becomes a consumer report.⁵
- (4) Public record information obtained by a CRA and reported (in whole or in part) to an employer client is a consumer report, subject to provisions of the FCRA, summarized in the next section.

2. Consumer Reporting Agency Responsibilities under FCRA

FCRA Responsibilities of a CRA/Pre-employment Screening Firm

The FCRA places a number of duties on CRA’s who report criminal history information about an applicant to employer clients:⁵

1. FCRA 607(a) requires every CRA to maintain “reasonable” procedures designed to avoid violations of FCRA 605 (relating to what may be reported) and FCRA 604 (relating to permissible purposes). Employment screening is a permissible purpose under FCRA 604. FCRA 605 contains a limitation of seven years on criminal information other than convictions, such as arrests.⁶ In other words, a criminal history search can reveal too much information, information that although known to a CRA is impermissible for a CRA to share with its employer client. For example, a criminal history database search may reveal an arrest that cannot be reported under the FCRA because it is more than seven years old or is not permitted to be considered for employment purpose under some state law. The database search may also reveal other records where an applicant was later

⁵ See FTC staff opinion letter (LeBlanc, June 9, 1998).

⁶ Although the seven-year limitation on reporting convictions was removed from the federal statute in 1997, it arguably remains effective as a limitation in a number of states, including California. If a screening firm reported a criminal matter based only upon a database hit that was not in fact proper to report under state law, there could be legal consequences.

pardoned, or the case had some other disposition that would prevent an employer from utilizing the information for employment purposes.

2. FCRA 607(b) requires every CRA to follow “reasonable procedures to assure maximum possible accuracy” of the information concerning the individual as presented in a consumer report. For example, if a record that purportedly matches the applicant were reported from a proprietary criminal history database directly to an employer, and any of the information was in fact wrong or was not related to the particular applicant, either or both the database vendor (if it is a CRA, as discussed below) and the pre-employment screening CRA that reported the information to an employer client might have to prove in court that its procedures to comply with the law were reasonable.⁷

If public record information is reported, the words “maximum possible accuracy” in FCRA 607(b) apply not only to the information itself, but also to whether the information is in fact about the applicant. If, for example, a search of a criminal history database requires only a name match, the information should never be reported by a CRA without matching some the record to some other personal identifiers of the subject. In many instances, the only way to determine the identity of the subject of a court or other public record is to pull the file itself to look for matching identifiers such as date of birth, SSN, or driver's license number. If those identifiers are all missing from the record, it may not legally be possible to report the information as a match.⁸

3. FCRA 607(d) requires that every CRA provide its clients (no matter whether the client is an employer client or another CRA) with the notice prescribed by the FTC.⁹

4. If criminal history information is included in a consumer report to an employer client, FCRA 613 requires the CRA to conform to one of the following alternatives:

(a)(1) Directly notify the applicant that public record information about her is being reported to the employer client.

(a)(2) Follow “strict procedures designed to insure” that the information is complete and up to date. Criminal information can be considered up to date only if the current public record status of the item is known at the time the report is made. Essentially, this

⁷ It is not legally necessary that the consumer report be entirely complete or correct, but only that the procedures used to compile the data and to identify it with the subject were themselves reasonable.

⁸ **A “Reasonable Procedure” under Section 607(b)**

Here is the way one competent CRA decides whether to report a criminal record to its employer client. The facts available to be compared are: First name (1), last name (2), date of birth (3), SSN (4), and gender (5):

Matches	Action
1, 2, 3, 4	Report
1, 3, 4	Report
1, 2, 3, 5, 6 of 9 numbers in SSN	Report
1, 2, 3, 5, SSN blank, last name not common	Report
Any other	Do not report

⁹ See <http://www.ftc.gov/os/statutes/2user.htm>.

alternative requires a CRA to search the actual court case, arrest or other information at its source.

5. If criminal history information is procured by a CRA from another CRA for the purpose of reporting all or part of the information directly to an employer client, FCRA 607(e)(1) requires the buyer CRA to inform the seller CRA of the identity of the employer client and the permissible purpose for which the report is to be obtained.¹⁰

3. Employer Responsibilities under FCRA and Other Law

Employers have three choices in obtaining public record information such as criminal history records:

- (1) **Do it yourself—by mail, phone or in person**—In this scenario, employees of the employer must go directly to the government agency that is the source of the information.¹¹ By going this route, the employer avoids altogether being subject to the FCRA.
- (2) **Do it yourself—search a government agency database**—As mentioned above, some courts and state central repositories make their data available online. This access method is merely an extension of the first choice for the purposes of this article, and the employer still avoids being subject to the FCRA, as long as the source is a database provided directly by the government agency, not by any intermediary.
- (3) **Use an intermediary**—Rather than going through all the trouble of doing these checks, an employer can hire someone else to get the information.

If an employer is dead set on avoiding the FCRA with respect to criminal history information, it will need to use only the first or second methods to obtain these kinds of records. Even so, the use of intermediaries to obtain other, public or non-public information will still subject the employer to some provisions of the FCRA.

If, on the other hand, an employer hires any intermediary to obtain public record or any other information about an applicant or employee, that intermediary is—subject to the LeBlanc exception—a CRA,¹² and the employer is subject to the FCRA.

Employers' Responsibilities under FCRA

In addition to an employer's general responsibilities to obtain the permission of an applicant or employee before obtaining any consumer reports and to disclose certain other activities related to obtaining consumer reports, an employer who uses information such as a criminal history information obtained through a consumer report, the employer

¹⁰ FCRA 607(e)(2) also places requirements on the selling CRA, such as a proprietary criminal history database vendor.

¹¹ There is one small exception to this rule explained in an FTC opinion letter (LeBlanc, June 6, 1998) if the employer uses a local individual to obtain the records on its behalf, but we recommend not depending on this exception to protect an employer from FCRA complaints.

¹² Whether or not the outside agency thinks or admits that it is a CRA, it is. Even an attorney firm can be a CRA. You cannot depend on the outside agency to be conversant with the FCRA. Therefore, an employer should take responsibility to know the FCRA requirements that apply to a CRA as well as to the employer itself. Needless to say, using a competent, FCRA-compliant pre-employment screening firm is an employer's best protection.

has specific responsibilities under FCRA **if it uses the criminal history information as a factor in denying employment to an applicant or in dealing adversely with a current employee.** In these instances, FCRA 604(b) requires an employer:

- (1) before taking “adverse action,” to provide the applicant or employee with a chance to dispute any information in a consumer report that is a factor in taking the action, and
- (2) after taking the action, providing further information to the applicant or employee, based on FCRA 615.

Employer Responsibilities under Other Law

Other employment laws also place legal liability on employers, as follows:

1. Lack of diligence—An employer who relies on its own search of a criminal history database could face exposure if a criminal record was missed when a traditional courthouse search by a competent pre-employment screening firm would have easily found it.

2. Incomplete data—An employer risks legal action if it makes adverse employment decisions based upon a proprietary criminal history database without confirming identity or ensuring that the information is complete and up to date.

3. Impermissible use of data—Another critical issue for employers who purchase public record information directly or indirectly is the legal use of the information under the Equal Employment Opportunity Commission (EEOC) rules concerning the use of criminal records. Under EEOC rules, an employer may not deny employment to an ex-offender unless it is a business necessity, determined by reviewing the following three factors:

- (1) The nature and gravity of the offense.
- (2) The amount of time that has passed since the conviction or completion of sentence.
- (3) The nature of the job being held or sought.

Unless an employer has pulled information from a primary source, such as the actual court records, it may not be able to make this determination.

4. Use of arrest records and other impermissible records—Many public record and proprietary databases are compiled from records provided by law enforcement or correctional authorities, not by courts. These records contain arrest information, which may not explain what, if anything, happened in court. In this instance, an employer needs to be aware if its state has a prohibition against considering arrests not resulting in convictions. For example, in California it is a misdemeanor for an employer to obtain or consider arrests records in employment decisions that did not result in a conviction or is not a pending case; an employer may only rely on convictions or pending cases. Even if a state allows consideration of arrest records, under the EEOC rules an employer must independently verify the underlying behavior and may not use an arrest all by itself as an indication of lack of fitness. The critical determinant is the behavior, not the police record.

Relying only upon a database report of an arrest without independent verification leaves an employer vulnerable to legal liability. Some states have special rules about the use of certain misdemeanors or cases that resulted in some sort of special disposition, such as

pre-trial diversion. There are also limits on the use of cases that have been judicially eradicated from the record following probation, or where a governor's pardon has been granted.

Should an Employer Try to Avoid Using a CRA?

There are certain circumstances, mentioned above, in which an employer can obtain more information for itself than a CRA can obtain for it. In those instances, an employer may want to go directly to the government source, such as a statewide criminal history repository. However, because of the practical difficulty in doing applicant or employee background checks itself, **we believe it is best practice for every employer:**

- (1) To utilize a competent pre-employment screening firm for its expertise in locating and interpreting public and non-public information, and**
- (2) to always assume that it is subject to the FCRA, and treat applicants accordingly.**

By operating under FCRA rules, an employer does not tread in the treacherous waters of potential invasion of employee privacy. The FCRA is a more or less fixed standard that defines the responsibilities and rights of parties involved in screening. Employers who do it themselves are controlled by more ambiguous "privacy" rules. In addition, employers who do screening themselves may well find that they invoke the FCRA anyway by inadvertently using FCRA-compliant sources. For these reasons employers normally find that the best protection is to operate under FCRA rules.

4. New Method of Screening for Criminal History

In contrast to going to the source information at each individual courthouse and at each individual state depository, there is a new and evolving method for conducting criminal history background checks, using **online, proprietary criminal history databases**. The firms selling access to these databases claim the databases contain millions of criminal records, and that searches of these databases cast a much wider net in addition to being both quick and inexpensive. However, these new database searches create significant issues and opportunities for employers and pre-employment screening firms alike.

Criminal History Database Shortcomings

All criminal history databases, whether public or proprietary, have obvious shortcomings.

- 1. Geographic Coverage**—First, recognize that there is no such thing as a truly "national" criminal history database available to the public. In addition, as discussed below, most statewide databases, whether compiled by government or by a private vendor, are way short of being truly statewide in some respect.
- 2. Disclosure**—Both database vendors and CRA's that use these databases must be very clear in their marketing and contracts not to mislead their customers to believe that they are receiving a service that does not exist. CRA's that make such a claim are risking legal liability in the event a criminal is hired after a search of a statewide or "national" database failed to uncover a criminal record.
- 3. Completeness**—A database can be incomplete for a number of reasons. First, not all statewide repositories contain complete records from all counties in the state. Second, the records that are actually reported may be incomplete or lack sufficient detail about the offense or the subject for reporting purposes. Third, some databases contain only felonies

or contain only offenses where a state corrections unit was involved. Fourth, the database may not carry subsequent information, such as a pardon or some other matter that could render an item not reportable under the FCRA. Finally, statewide databases may not include any federal court information.

4. Accuracy—Database searches are only as good as the information entered into the database. If a particular county or correction authority makes a data entry error in the subject's name, it can lead to a false negative report, hiding a criminal record that does exist.

5. Name Variations—An electronic search may not be able to recognize variations in subject names that a person would notice in looking at the agency's index. The applicant may have been arrested under a different first name or some variation of first and middle name. A female applicant may have a record under her maiden name.

6. Timeliness—Records in a central repository are always stale to some extent. First, as mentioned above, there is the lag time before the reporting agencies submit the data. Then the statewide repository may only enter new data at intervals. Some states, for example, only update information quarterly. This means that the most current offenses are the ones least likely to appear in a search of statewide databases. The only exception to this rule would be online court record systems, like PACER for federal courts.

Criminal History Database Benefits

On the other hand, traditional criminal history searches have inherent limitations searches of criminal history databases can overcome to some extent:

1. Time Delays—Traditional criminal record searches can take days or weeks before results are available. Online database searches are virtually instantaneous.

2. Expense—Some government agency searches are not only time-consuming, but also incur expensive official fees.

3. Geographic Coverage—Traditional on-site or online court searches can miss records because the applicant may have crossed county or state lines to commit her crime. Statewide searches of central criminal history repositories cast a much wider net, but still are only as good as the choice of states to search. A proprietary database may contain records from many states, all accessible in one search.

4. Court Coverage—Traditional on-site or online court searches can miss records because the crime was adjudicated in a court that was not searched. Proprietary databases compile information from many levels of courts.

5. Proprietary Criminal History Database Vendors

Database Compiled for a Non-FCRA Purpose

A CRA may have access to a criminal history database that was not compiled for employment screening purposes. As a general rule, whether or not the vendor contract contains any provision dealing with its use for FCRA purposes, the CRA should follow FCRA 613(a)(2), and never report information directly from a search of the database. However, we think these non-FCRA database vendors would be wise to be crystal clear with respect to this matter. For example, Merlin Information Services (www.merlincata.com), which provides databases of public record information used primarily for skip tracing, demands that its subscribers agree they will not use any

information obtained from Merlin directly as part of a consumer report. This agreement is reiterated on its web site whenever a subscriber logs on. The provision not only effectively invokes FCRA 613(a)(2), but also clarifies that Merlin is not in the business of assembling data for FCRA purposes in the first place.

Database Compiled for FCRA Purposes

Proprietary criminal history database vendors that compile their records for the purpose of supporting employment screening applications are subject to all the provisions of the FCRA that apply to CRA's. The contractual handling of the alternative provisions of FCRA 613(a) is crucial to whether such a vendor is FCRA-compliant.

Since criminal history database vendors assemble their information for FCRA purposes, they have a greater problem and responsibility than a vendor like Merlin. They should have two clearly distinct search protocols: one for CRA's doing an FCRA-compliant or prescreening search, and another for employer/end users. A prescreening search can only be performed by a CRA, but an FCRA-compliant search can be performed by either a CRA or an employer/end user.

1. Prescreening Search Protocol (FCRA 613(a)(2) Compliant)—A prescreening search protocol allows the user—who must also be a CRA—to enter as few personal identifiers as it wishes to limit matches to the database. The CRA might be allowed to enter only a name in order to search most broadly across all the statewide databases included in the criminal history database. The CRA must not report any of the resulting hits directly to its employer client. Rather, the CRA would then assess the matches to determine which might match the applicant name for follow-up as potential criminal history, and conduct actual searches of courts or other government agencies where the information originated, and apply the “strict procedures” under FCRA 613(a)(2) to determine whether to report the government agency search results to its employer client.

This type of broad search protocol should never be made available directly to an employer because of the restrictions imposed on CRA's by FCRA 607 as well as by FCRA 613(a)(2).

FCRA 613(a)(2) requires records reported to an employer client to be “complete and up to date.” Can the information from a criminal history database meet the standard of FCRA 613(a)(2)? The FTC staff says “No,” at least with respect to *proprietary* databases. The FTC staff when asked a question about “stored data public records,” meaning proprietary databases, provided what we think is the authoritative although unofficial answer in its opinion letter (Allan, May 5, 1999), issued more than three years ago:

“A CRA does not comply with FCRA 613(a)(2) “when it furnishes consumer reports for employment purposes that include negative public record information from stored data, without first verifying whether the information is complete and up to date.”

A footnote to this statement reads:

“Such CRA's may, of course, alternatively comply with the FCRA by adhering to the requirements of Section [613(a)(1)].”¹³

¹³ The opinion letter cites FCRA 613(1) and (2), which were redesignated (a)(1) and (a)(2) in the 1997 Clarification Act.

(The FTC staff opinion letter did not address the analogous issue of reporting information retrieved directly from a government agency criminal record database. CRA's traditionally report (1) violations found in state motor vehicle department databases—violations that have been reported by courts to motor vehicle departments—and (2) records reported by statewide criminal records repositories, without verifying that the record is either actually applicable to the subject, accurate, complete or up-to-date by obtaining the underlying record from the applicable court.)¹⁴

Record vs. Index

Because a proprietary criminal history database is compiled from many different sources, the extent of the information associated with a name may vary considerably. The case records from a court may contain a full summary of docket information about a case, including its disposition, whereas the case records from another court may contain only a docket number and date of final adjudication. This second type of record can be thought of as an index entry rather than a case record. An index entry must only be used as a prescreening tool and never reported by a CRA to an employer client as raw information. Since index entries may be misunderstood, they should be made available to employers by a proprietary database vendor only under clear contractual limitations?

2. FCRA Compliant Search Protocol (FCRA 613(a)(1) Compliant)—Either a CRA or an employer may utilize this type of search protocol, if the contract with the proprietary database vendor requires compliance with FCRA 613(a)(1). In this type of search protocol, reports of the results of the search of the database are available to an employer without further research, as long as the CRA (which may be either the database vendor CRA or the pre-employment screening CRA) also informs the applicant directly if public record information is found and reported to the employer.

If the user is an employer, the vendor must itself determine the minimum standard to be applied to find a match on its database depending on the name and personal characteristics entered. Such a standard is necessary to conform to FCRA 607(a) and (b). This standard should be programmed into the kind of rules illustrated in footnote 8 above. The vendor is also then responsible for the 613(a)(1) report to the subject if any matching records are found.

If the user is a CRA, the database vendor matching standard may be looser than the standard that its CRA user might apply to the resulting matches before reporting to its employer client, but only with the understanding that the CRA/user will further narrow the results before forwarding them to its employer client. The CRA user is not required to report all the hits it receives from the database search, and may want to use some of the matches as leads for court searches rather than merely reporting the search results to its employer client.

Who Are the Major Proprietary Database Vendors?

We have provided the foregoing, extensive background about the application of FCRA to public and proprietary criminal history databases so that CRA's and employers can make

¹⁴ Although traditionally results of a statewide criminal history repository are reported without verification, it is, we suppose, possible to argue that reporting court information from a statewide repository compiled after the fact from court records without verification at the court itself also runs afoul of FCRA 613(a)(2), but such an argument is beyond the scope of this article.

reasonable decisions about whether, when and how to use the databases provided by vendors today.

Although there may be many regional vendors, we will limit our attention to three national vendors that have recently been competing in marketing their web-based, proprietary criminal history databases to pre-employment screening firms and/or employers.¹⁵ They are:

- ChoicePoint (www.choicepointinc.com)—National Criminal File
- National Background Data (www.nationalbackgrounddata.com)—National Background Directory
- Rapsheets.com (www.rapsheets.com)

Although each of these vendors states that its product is FCRA-compliant, each interprets what that might mean quite differently. For example:

Who can access?

ChoicePoint National Criminal File—accessible only by ChoicePoint employer clients.

National Background Data—accessible only by CRA “affiliates.”

The Rapsheets databases—accessible by anyone.

How do you get access?

ChoicePoint National Criminal File—Call an 800 number for more information. (Prior to sometime in 2002, you could print out an application and contract from the web, complete it and fax it back for approval.) Contract no longer available on web site.

National Background Data—Complete an online application. Contract not available on web site.

The Rapsheets databases—Click agreement to online contract for immediate access.

Does vendor admit to being a CRA?

ChoicePoint—Yes.

National Background Data—Yes.

Rapsheets—Yes, but one version of contract admits the site is a CRA while the other says the site is “arguably” a CRA.

¹⁵ **A Little History**—Our research indicates that the first FCRA-compliant criminal records database was compiled by DAC Services, Tulsa, OK (www.dacservices.com) around 1993. DAC is a national employment screening firm specializing in the transportation industry. DAC includes a criminal records search as part of its highly evolved “Recommended Hiring Program” for the transportation industry. DAC does not promote its database capability, but does comply with all the procedures we recommend, including:

- (1) carefully avoiding misrepresenting that their criminal records search is “nationwide” or “national,”¹⁵
- (2) applying rigorous logic to its database search in order to eliminate matches that do not meet the reasonableness test of section 607(b) (false positives)
- (3) sending a section 613(a)(1) notice to the applicant at the address provided by its employer/client whenever a search of its database discloses a criminal record that DAC intends to report.

Do they mention in their contracts the requirements of FCRA 613?

ChoicePoint—Current contract not available. Prior contract does not specifically mention whether ChoicePoint will follow FCRA 613(a)(1) requirements.

National Background Data—Yes. CRA affiliate agrees to notify applicant according to FCRA 613(a)(1) if it wishes to use that option.

Rapsheets—No mention of FCRA 613 requirements.

Consumer disclosure rights under FCRA 609?

Consumers have rights under FCRA 609:

(1) to find out what is on file about them in the records of a CRA¹⁶ and

(2) to find out who has conducted a search for criminal history records about them.

Here is how these three services handle FCRA Section 609:

ChoicePoint—No indication on web site of consumer right to receive a report on herself.

National Background Data—Consumer contact address and telephone number provided on web site. As indicated on its web site, this vendor will provide a report for a consumer on herself and a list of any affiliates that have conducted a search for records about the consumer.

Rapsheets—No consumer information on web site.

6. The Big Questions

Since these vendors do not agree about how the FCRA applies to the use of their databases, pre-employment screening firms and employers are left to decide for themselves whether, when and how to use proprietary criminal history databases and which vendor(s) to contract with.

Here are some of the crucial questions you need to answer before making a decision about this valuable new source of criminal history information:

- A. Should employers and/or CRA's consider employing these proprietary criminal history databases at all?**
- B. Are employers and/or CRA's that do not take advantage of these criminal history databases failing to exercise proper due diligence in the screening of an applicant?**
- C. Are these proprietary criminal history databases truly FCRA-compliant?**
- D. If the databases are FCRA-compliant, are the vendor contracts adequate to protect the vendor itself, their clients and consumers according to the provisions of the FCRA?**
- E. What precautions do employers need to take if they use proprietary criminal history database information directly from the vendor database in making an employment decision?**
- F. What issues should proprietary criminal history database vendors reconsider?**

¹⁶ See www.banko.com for an example of a web site that contains what we think is the minimum level of consumer information.

The remainder of this article will discuss each of these questions, detailing the ramifications of using these databases in order to help pre-employment screening firms, employers and the database vendors themselves answer these and related questions.

A. Should employers and/or CRA's consider employing these proprietary criminal history databases at all?

On the one hand, neither a direct search of a statewide criminal history repository nor a search of a proprietary criminal history database can be assumed to meet the same level of detailed due diligence as a search of actual court records. On the other hand, searching only in actual courts or in particular statewide repositories limits the scope of the search to a narrow geographic area and may take quite a long time to obtain results. As the proprietary vendors point out, a search of a proprietary criminal history database compiled from many states and many sources provides both a faster initial search and much broader geographic coverage at a fraction of the cost of going to the many possible source government agencies.

We conclude that as long as the shortcomings of these databases are recognized, they can provide a breadth of useful information that direct searches of court records can never achieve. A determination of which of the available databases is most extensive is beyond the scope of this article.

B. Are employers and/or CRA's that do not take advantage of these criminal history databases failing to exercise proper due diligence in the screening of an applicant?

If a search of a proprietary criminal history database is "useful," is it also legally "necessary"? It can be argued that in a society where people move 3,000 miles all the time a CRA's or employer's failure to utilize a database with broader geographic coverage than searches of local courts and statewide databases is "negligent" because the information is readily available and casts a much wider net than traditional criminal history searches.

To our knowledge, this argument has not yet been the subject of litigation. Still, each CRA and employer should consider the risk from not spending a few extra bucks for a broad search.

C. Are these proprietary criminal history databases truly FCRA-compliant?

Remember that these databases may be used in two different ways:

- (1) to generate leads, and
- (2) to directly generate reports to employers.

1. Lead Generation—We have concluded above that any old database can be used as a source of leads by a CRA as long as nothing from the database is directly reported by a pre-employment screening firm to an employer client.

2. Consumer Report—We have concluded that the results of a search of a proprietary criminal history database compiled for the purpose of providing information for pre-employment screening constitute a consumer report, except in the one instance discussed above when the information is used exclusively to generate leads for direct searches of courts or other government agencies.

The results of a direct search by an employer of a proprietary criminal history database compiled and marketed for use in pre-employment screening still constitutes a consumer report. Therefore, such a search should not be performed directly by an employer without assurance from the vendor that the vendor is not only FCRA-compliant in some general sense, but that the vendor specifically complies with all the provisions listed above in this article. In order for an employer to determine if a vendor complies with the FCRA, look for two features:

- (1) The vendor's search methodology should require reasonable matching of applicant identifying information such as SSN and date of birth so that false positives are minimized (FCRA 607), and
- (2) The vendor's contract should state that it will accept legal responsibility to inform the applicant if any hits are returned by an employer search (FCRA 613(a)(1)).

The results of a search by a CRA of a proprietary criminal history database compiled and marketed for use in pre-employment screening also constitutes a consumer report if reported to the employer. However, as noted above, if the report is only used to generate leads, and the results are not being passed along to the employer client, the pre-employment screening firm is then responsible to comply with the FCRA requirements noted above, including conformance with FCRA 613(a)(2), in its follow-up public record search based on the results.

If on the other hand the CRA wants to share directly with its client the information gleaned from a search of the proprietary criminal history database, the CRA can do so if it conforms to FCRA 607 and 613(a)(1).¹⁷ In order for a CRA to determine if a vendor complies with the FCRA, look for two features:

- (1) The vendor's contract should list all the applicable FCRA provisions mentioned in this article, and
- (2) The vendor's contract should specifically require the CRA to comply with FCRA 613(a)(1).

D. If the databases are FCRA-compliant, are the vendor contracts adequate to protect the vendor itself, their clients and consumers according to the provisions of the FCRA?

Database Vendor Contracts

As noted above, the vendor contracts should contain certain specific terms, especially with respect to the matching of database records to the applicant.

¹⁷ This would be required whether or not the database vendor contractually requires the CRA to conform to this FCRA provision. We have also concluded that this is a resale of a consumer report, which makes FCRA 607(e) applicable to the report as well.

Prescreening v. Consumer Report (Using FCRA 613(a))

The identity problem—that is, does a particular criminal history record apply to a particular applicant—is one of the most frustrating problems for a CRA to resolve as it tries to match criminal history and other public record information to the identifying information about an applicant. On the one hand, the CRA wants to report everything that might be about the applicant; on the other hand, the FCRA requires “reasonable” and/or “strict” procedures to assure the information reported is reasonably connected to that applicant.

This frustration is exacerbated by the fact that court and other criminal history record systems were not designed to assure that personal identifying information, such as date of birth and SSN, is accurate. In fact, smart criminals might just make a practice of consistently giving the same, wrong personal identifying information when arrested.

FCRA 613(a) seems to recognize the difficulties inherent in matching this kind of public record information to any particular individual. We interpret the provision as striking a balance by saying in FCRA 613(a)(1) that if the CRA is not entirely sure that the information is applicable to this applicant or that it may not be up to date, the information may still be reported to the employer as long as the employer agrees contractually with the CRA that the applicant will be informed by the CRA that some public record information that may be about the applicant has been reported to the employer,¹⁸ thereby giving the applicant notice so that she can challenge the accuracy of the information.

CRA’s have traditionally ignored the FCRA 613(a)(1) option, and adhered (or say they adhere) to the strict 613(a)(2) standard with respect to criminal history records, possibly because they are uncomfortable about asking permission of their clients to make the required consumer disclosure under FCRA 613(a)(1). However, we suggest that this option (1) might be useful to an employer client through its CRA because it would allow the CRA to report information directly from proprietary criminal records database in many circumstances.

CRA Contracts

A CRA that uses a proprietary criminal records database needs to abide by two contracts in its operations:

- (1) its contract with the proprietary database vendor, and
- (2) its contract with its employer client.

The CRA and its employer client need to be aware of the provisions of each contract that deal with the FCRA 613(a) options.

1. CRA/Database Vendor Contract

A proprietary database vendor contract may contain one of three types of provisions with respect to FCRA 613(a):

- (1) The contract may be silent.

¹⁸ It is interesting that the CRA is not required to provide the information or to characterize the information as adverse, but only to notify the applicant of the fact that some sort of public record information was found and reported to the employer.

- (2) If the database was compiled for employment verification or other FCRA purposes, the contract may specify that the CRA user may report results directly if it complies with the FCRA 613(a)(1) procedures.
- (3) If the database was not compiled for employment verification or other FCRA purposes, the contract may require the subscriber to adhere to the FCRA 613(a)(2) rule.

Therefore, a CRA would expect that the database vendor would have something to say about how it handles this provision. However, the contracts of two to the three vendors are silent on the subject.

One of the vendors, National Background Data (NBD) only sells to or through employment screening firms. Its contract demands that subscribers follow the disclosure provision of FCRA 613(a)(1) if they choose to report information directly from the database. Further, this vendor applies its own matching logic to searches by its subscribers to limit the matches to meet its responsibility under FCRA 607(b) to “follow reasonable procedures to assure maximum possible accuracy” of the information provided.

The second vendor, ChoicePoint, only sells access to its data to employers, directly or through resellers, but not to CRA’s for their own use. As a CRA, it seems to us that it should be subject to FCRA 613(a)(1). We do not know its position on this issue. In recognition that it is subject to FCRA 607(b), we understand that ChoicePoint like NBD applies matching logic to searches by its subscribers.

The third vendor, Rapsheets, does not appear to address this issue in the contract reviewed for this article.

CRA/Employer Contracts

Who should make the final decision about whether a CRA is to utilize FCRA 613(a)(1) or 613(a)(2) in its reporting to an employer client, the CRA or the employer client? Until today, we know of no contracts between CRA’s and employer clients that address this issue at all. Nor do we know of any CRA other than DAC Services that utilizes FCRA 613(a)(1) as a business method. As a consequence, the default position of other professional firms in the pre-employment screening industry has been as follows under FCRA 613(a)(2):

- (1) Statewide Official Criminal Record Databases—Consider the information in the database correct and up-to-date, and report information from records that meet the CRA’s matching criteria.
- (2) Proprietary Criminal Record Database—Consider database information as a lead, research the underlying, original record, and report only public records that match the applicant according to the CRA’s matching criteria. Any CRA that reports information directly from such a database without verification is ignoring the requirements of the FCRA.

Should the contract between a CRA and an employer client address the issues involved in the use of public record and proprietary criminal record databases? We conclude that any CRA that wishes to help its client take advantage of FCRA 613(a)(1) should delineate the procedures in its contract with its employer clients. Alternatively, because of the issues

raised by FCRA 613(a)(1), a CRA may want its contract with an employer to reflect that proprietary databases will be used only as a prescreening tool, and that nothing, including a “clear” report, will be reported to the employer based on a search of a proprietary database. As another alternative, the contract may stipulate that the CRA will report a “clear” indication from the proprietary database search, with the understanding that such a report does not constitute a finding that the record of the applicant is in fact clean.”

E. What precautions do employers need to take if they use proprietary criminal history database information directly from the vendor database in making an employment decision?

Two of the vendors mentioned above sell criminal history database searches directly to employers. The third vendor, National Background Data, has decided not to sell directly to end-user employers, but only to and through CRA’s. There are a number of potential landmines for employers if they perform these searches themselves as part of their pre-employment screening program. We have discussed these issues above, and have concluded that employers should consider carefully the potential liability that may arise from do-it-yourself searching using a proprietary criminal history database.

F. What issues should proprietary criminal history database vendors reconsider?

We have discussed above a number of issues that apply to how we think proprietary criminal records database vendors should conduct themselves in an FCRA-compliant manner. Vendors of these proprietary databases also need to reconsider their marketing promotions, educational responsibilities, legal responsibilities, contractual provisions, and consumer services based on the concerns of employers and of CRA’s, as discussed in this article.

1. Marketing—Vendors need to be very careful about making sure their employer and screening firm prospects and clients understand the exact nature and limitations of the data provided in each state, and the meaning of “national.”

2. Education—These databases are a new and valuable tool, but are easily subject to misuse without proper training of the people who are going to use the information. Vendors need to mount educational programs to assure that users understand legal and practical limitations in using the information provided.

3. Legal Responsibility—Each of the vendors discussed in this article act as a CRA. Any non-CRA activities of these vendors should be identified clearly so that users are aware when the vendor is acting as CRA’s and when it are not, when reports are consumer reports and when the reports are not. In any event, we believe that separate contracts are necessary for different customer types (employer, investigator or CRA) and for different purposes, to clearly invoke the differing FCRA requirements that apply to each type.

4. Contracts—Contracts need to include sufficient references to all the applicable provisions of FCRA—including 607(a), 607(b), 607(d), the applicable part of 613, and possibly 607(e)—as well as to other laws that may apply to use of the information. Any

legal disclaimers in contracts should match the reasonable customer expectations created by the marketing and sales efforts.

5. Consumers—We think that vendors are not only responsible to provide information to consumers about any searches done on them in the vendor's criminal history database, but also to be prepared to perform a search on behalf of any consumer who provides adequate information to identify her according to the matching logic used by the vendor. Vendors should add consumer-related FCRA information to their web sites.

7. Conclusions

We have looked at the issues raised by the availability of online, proprietary criminal history databases from the point of view of the vendors that provide them, the CRA/pre-employment screening firms that use them, and the employers who either use them or obtain information through CRA's from them.

We have concluded that such databases are a potentially useful and legal tool for employers and their agents to use, as long as each kind of user understands:

- (1) the inherent limitations of the information in these databases,
- (2) the inherent liabilities under FCRA and other federal and state laws for misuse of information garnered from these databases,
- (3) the necessity of also performing actual searches in actual courts to verify criminal case information unless FCRA 613(a)(1) is invoked, and
- (4) The necessity of contractual provisions among vendors, CRA's and employer clients to determine how information may be reported.

Whether or not the proprietary criminal history database vendors come to grips with the issues raised in this article, CRA's and employers should use the information obtained from these databases with great care to assure compliance with the letter as well as the spirit of the FCRA.

About the authors:

Lester S. Rosen (lrsr@esrcheck.com) is an attorney at law and President of Employment Screening Resources (ESR), a national background screening company located in California (www.ESRcheck.com). He is a consultant, writer and frequent presenter on the Fair Credit Reporting Act (FCRA), pre-employment screening and safe hiring issues. He is a certified specialist in criminal law in California, a former deputy District Attorney and defense attorney, and has taught criminal law and procedure at the University of California Hastings College of the Law. His jury trials have included murder, death penalty and federal cases. He graduated UCLA with Phi Beta Kappa honors in 1973, and received a J.D. degree from the University of California at Davis in 1976, serving on the Law Review. He has qualified and testified in court as an expert in the area of safe hiring and pre-employment background screening.

Carl R. Ernst (carl.ernst@ernst.cc) is an editor and publisher of information about public records. He is a principal in BRB Publications (www.brbpub.com), the leading publisher of information about where and how to access public records at the local, state and federal levels of government. He has studied and written about the Fair Credit Reporting Act for many years, focusing on the implications of the 1996 and 1997 amendments to creditors and employers. He is also the CEO of Ernst Publishing CO., LLC (www.ernst.cc), which specializes in providing information to assist financial institutions in the preparation, filing, recording and searching under Article 9 of the Uniform Commercial Code (UCC filings) and real estate law (deeds, mortgages, and related instruments).