# BROKEN RECORDS

## HOW ERRORS BY CRIMINAL BACKGROUND CHECKING COMPANIES HARM WORKERS AND BUSINESSES


NCLC®
NATIONAL
CONSUMER
LAW
CENTER®

April 2012

## ABOUT THE AUTHORS

**Persis S. Yu** is a staff attorney at the National Consumer Law Center (NCLC) who focuses on the Fair Credit Reporting Act, student loan law, and other consumer credit issues. Prior to joining NCLC, Persis was a Hanna S. Cohn Equal Justice Fellow at Empire Justice Center in Rochester, New York. Her fellowship project focused on credit reporting issues facing low-income consumers, specifically in the areas of accuracy, housing, and employment. Persis is a graduate of Seattle University School of Law, and holds a Masters of Social Work from the University of Washington and a Bachelor of Arts from Mount Holyoke College.

Contributing Author **Sharon M. Dietrich** is the Managing Attorney in Community Legal Services of Philadelphia's Employment and Public Benefits Units. She specializes in employment issues faced by ex-offenders and unemployment compensation issues. Ms. Dietrich has been presented numerous awards for her work, including the 2006 Kutak-Dodds Prize from the National Legal Aid and Defender Association, the Civil Legal Aid Attorney of the Year Award from the Pennsylvania Bar Association (2006), and the Andrew Hamilton Award from the Philadelphia Bar Association (2005). Prior to her employment with CLS, Ms. Dietrich served as law clerk for Ann Aldrich, U.S. District Judge for the Northern District of Ohio. Ms. Dietrich is a summa cum laude graduate of Albright College and a graduate of the University of Pennsylvania Law School.

## ACKNOWLEDGMENTS

The authors thank Maurice Emsellem, Madeline Neighly, and Michelle Rodriguez of the National Employment Law Project; Lisa Bailey and Patricia Warth from the Center for Community Alternatives; Christopher Wilmes of Hughes Socol Piers Resnick & Dym, Ltd.; and many others for providing their valuable time and expertise on this subject. We also thank NCLC colleagues Carolyn Carter, Jan Kruse, and Chi Chi Wu for valuable comments and assistance, and Deborah Durant for research assistance.

The findings and conclusions presented in this report are those of the authors alone.

NCLC®
NATIONAL CONSUMER LAW CENTER®

## ABOUT THE NATIONAL CONSUMER LAW CENTER

Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and disadvantaged people, including older adults, in the U.S. NCLC advances economic fairness through policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services; and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitive practices and help financially stressed consumers build and retain wealth.

# BROKEN RECORDS

## HOW ERRORS BY CRIMINAL BACKGROUND CHECKING COMPANIES HARM WORKERS AND BUSINESSES

## TABLE OF CONTENTS

# EXECUTIVE SUMMARY

Since 2007, the United States has experienced the worst unemployment rates since the Great Depression. Adding to this job crisis, criminal background checking companies are making it even more difficult for workers to obtain employment. Approximately ninety-three percent of employers conduct criminal background checks for some potential applicants, and seventy-three percent of employers conduct criminal background checks for all potential applicants. The widespread dissemination of criminal record histories limits employment opportunities for an estimated sixty-five million adults (nearly one in four adults) in the United States who have some sort of criminal record.

Moreover, criminal background checks often contain incorrect information or sealed information. Samuel M. Jackson was allegedly denied employment after a prospective employer ran an InfoTrack background check. InfoTrack reported a rape conviction from 1987—when Mr. Jackson was four years old. The rape conviction actually belonged to fifty-eight-year-old male named Samuel L. Jackson from Virginia, who was convicted of rape in November 18, 1987. That Samuel Jackson was incarcerated at the time the InfoTrack report was run.

Whether these checks should be used for employment screening is a matter of public debate. However, there is little debate that if these records are to be used, they *must* be accurate.

Despite its promotion as a public safety service, the sale of criminal background reports has become a big business generating billions of dollars in revenue. The Internet has facilitated the emergence of scores of online background screening companies, with many claiming instant access to millions of databases.

Under the Fair Credit Reporting Act (FCRA), background checking agencies are required to maintain procedures to ensure the accuracy of information they report about consumer. Unfortunately, the FCRA, as currently interpreted and enforced, fails to adequately protect consumers when it comes to employment screening. Even applicants who successfully remove errors from their background check are frequently denied employment.

Despite the importance of the accuracy of criminal background reports, evidence indicates that professional background screening companies routinely make mistakes with grave consequences for job seekers.

This report describes a number of ways in which background screening companies make mistakes that greatly affect a consumer's ability to find employment. Although the mistakes discussed in this report are not inclusive of all errors found on background checks, attorneys and community organizations that work with consumers with faulty background reports state that they repeatedly see background reports that:

- Mismatch the subject of the report with another person;
- Reveal sealed or expunged information;

- Omit information about how the case was disposed or resolved;
- Contain misleading information; and
- Mischaracterize the seriousness of the offense reported.

Many of these errors can be attributed to common practices by background screening companies, such as:

- Obtaining information through purchase of bulk records, but then failing to routinely update the database;
- Failing to verify information obtained through subcontractors and other faulty sources;
- Utilizing unsophisticated matching criteria;
- Failing to utilize all available information to prevent a false positive match; and
- Lack of understanding about state specific criminal justice procedures.

Even the National Association of Professional Background Screeners agrees there are some simple procedures that background checking companies can take to enhance the quality of their information. Unfortunately, few companies actually are willing to commit to even the limited recommendations of their own trade association. Criminal background checking is big business, and ensuring accurate and complete information reduces profits.

Based upon the issues identified in this report, we recommend that the Consumer Financial Protection Bureau (CFPB) use its rulemaking authority under the Fair Credit Reporting Act to:

- Require mandatory measures to ensure greater accuracy.
- Define how long an employer has to wait in between sending an initial notice and taking an adverse action, i.e., rejecting an applicant or terminating an employee.
- Require registration of consumer reporting agencies.

The Federal Trade Commission should use its FCRA enforcement authority to:

- Investigate major commercial background screening companies for common FCRA violations.
- Investigate major, nationwide employers for compliance with FCRA requirements imposed on users of consumer reports for employment purposes.

Finally, as the source of most of the data reported by background screening agencies, states have a huge role to play in ensuring the accuracy of criminal background checks. States should that ensure that state repositories, counties, and other public records sources:

- Require companies that have subscriptions to receive information by bulk dissemination from court databases to have some procedure for ensuring that sealed and expunged records are promptly deleted and ensure that dispositions are promptly reported.

- Audit companies that purchase bulk data to ensure that they are removing sealed and expunged data and, if a company fails such an audit, revoke its privilege to receive bulk data.

With the explosive growth of this industry, it is essential that the "Wild West" of employment screening be reined in so that consumers are not guilty until proven innocent. Currently, lack of accountability and incentives to cut corners to save money mean that consumers pay for inaccurate information with their jobs and, thus, their families' livelihood.

## Table 1 WHO CAN REIN IN FAULTY BACKGROUND SCREENING REPORTS?

Background screening companies routinely make mistakes when issuing criminal background checks. The result? Job seekers pay with their livelihood, while employers waste money and potentially miss hiring qualified employees as the result of sloppy work that skirts the Fair Credit Reporting Act (FCRA). This list contains common errors or bad practices found in reports from all corners of the United States. Adoption of the suggested remedies would greatly increase accuracy on reports by improving accountability.

| Inaccuracy/Poor Practice | Solution | Responsibility |
|---|---|---|
| Report Includes Sealed or Expunged Records | Develop procedures to ensure that purchasers of bulk public data delete sealed and expunged records, and perform audits to ensure compliance. | State legislatures, administrative agencies, and/or courts |
| Mismatched Report (providing a report on the wrong person) | Provide guidelines on matching criteria; require consumer reporting agencies to use all available data; and prohibit name only based matching. | Consumer Financial Protection Bureau (CFPB) |
| Incomplete Record (i.e., omits disposition data) | Requiring verification and updating of criminal records that lack disposition data for records more than one year old. | CFPB |
| Misleading Reporting (i.e., a single charge listed multiple times) | Prohibiting multiple reports of the same case regardless of source. | CFPB |
| Inability Of Applicant/ Employee to Correct Errors in the Report Prior to an Adverse Action | Require employers to allow sufficient time (i.e., 35 days) to fix report before taking adverse action. | CFPB |
| Screening Companies Disclaim Responsibility Under the FCRA | Require registration of all consumer reporting agencies and investigate major industry players for common FCRA violations. | CFPB and Federal Trade Commission (FTC) |
| Employers Fail to Provide FCRA Notices | Investigate employers for FCRA compliance. | FTC |
| Misclassifies Grade or Classification Of Offense | Investigate background screening companies for inaccurate reporting in violation of FCRA. | FTC |

## I. INTRODUCTION

Since 2007, the United States has experienced the worst unemployment since the Great Depression. During the month of March 2012 (the most recent data available), 12.7 million people remained unemployed.[1]

Adding to this job crisis, criminal background checking companies are making it even more difficult for workers to obtain employment. According to a 2010 survey by the Society for Human Resource Management, approximately ninety-three percent of employers conduct criminal background checks for some potential applicants, and seventy-three percent of employers conduct criminal background checks for all potential applicants.[2]

The widespread dissemination of criminal record histories limits employment opportunities for estimated sixty-five million adults (nearly one in four adults) in the United States who have some sort of criminal record.[3] There are many criticisms of this practice.

First, the use of criminal background checks disproportionately affects people of color. In fact, the Equal Employment Opportunity Commission (EEOC) has stated that denying employment based solely on the existence of a criminal history has a disparate impact on African Americans and Latinos.[4] African Americans account for 28.3 percent of all arrests in the United States, although they represent just 12.9 percent of the population; that arrest rate is more than double their share of the population. In contrast, the arrest rate for whites actually falls below their share of the population.[5]

Second, the widespread use of criminal background checks sets persons with criminal records up for future failure. Research demonstrates that the single greatest predictor of recidivism is the lack of stable employment.[6] Moreover, "providing individuals the opportunity for stable employment actually lowers crime recidivism rates and thus increases public safety."[7]

Third, background checks do not necessarily provide users with the information they think it does. There is little research that shows any correlation between the existence of a criminal record and the propensity to commit crimes at the workplace.[8] Furthermore, criminologists and practitioners agree that recidivism declines steadily with time clean.[9]

Finally, criminal background checks often contain incorrect information or sealed information.[10] Whether these checks should be used for employment screening is a matter of public debate. However, there is little debate that if these records are to be used, they must be accurate.

This report is focused on the last critique—accuracy. Currently, actual accuracy rates are not possible to obtain.[11] Commercial background checking companies are not required to be licensed, nor is there any one source identifying all of these companies. Therefore, as of 2012, there is no centralized location to obtain the kind of data required to generate accuracy data. Furthermore, as will be described in greater detail, too many employers fail to comply with notice requirements under the Fair Credit Reporting Act (FCRA). This hinders the ability to conduct a reliable survey of consumers to determine whether

they have been denied employment because of a commercial background check report. For these reasons, the focus of this report is on the types of problems found on background reports and the systematic practices that allow these inaccuracies to occur.

This report discusses in detail:

- Overview of the background check industry;
- The current laws in place to protect consumers;
- The types of problems often found on criminal background checks;
- Attempts by criminal background checking agencies to evade consumer protections;
- Ways that criminal background checking agencies could improve their procedures; and
- Recommendations for policy makers to improve protections for consumers.

## II. OVERVIEW OF THE INDUSTRY

### *A. Criminal Background Checks Are Big Business*

The rise in criminal background checks is in part due to employers' fears after the terrorist attacks of September 11, 2001. Immediately after September 11, commercial background check vendors reported significant increases in business.[12] Kroll, Inc. reported that the number of background checks it conducted increased twenty percent from 2001 to 2002.[13] ChoicePoint (now LexisNexis) reported that its monthly volume of background checks increased eightfold in the five months following September 11, 2001.[14]

Despite its promotion as a public safety service, the sale of criminal background reports has become a big business. In the company's decade of operation, ChoicePoint's annual revenue grew from approximately $400 million in 1997 to approximately $1 billion in 2008 before it was purchased by Reed Elsevier Group (the parent company of LexisNexis).[15] As a *BusinessWeek* article reported:

> Background screening has become a highly profitable corner of the HR world. At the screening division of First Advantage (FADV), based in Poway, Calif., profits soared 47% last year, to $29 million; revenue grew 20%, to $233 million. HireRight (HIRE), based in Irvine, Calif., reported that earnings jumped 44%, to $9 million, last year on revenues of $69 million. To grab a piece of this growing market, Reed Elsevier Group (RUK), the Anglo-Dutch information provider, agreed to acquire ChoicePoint for $4.1 billion in February—at a 50% premium to its stock price.[16]

In addition to the large national corporations, there are countless smaller local and regional companies providing criminal record information to local employers and property managers. Currently there are no licensing requirements to become a background checking agency and there is no system for registration. Thus, the total number of commercial reporting agencies currently operating is unknown. Anyone with a computer, an Internet connection, and access to records can start a background screening business.

## Largest Players in the Background Screening Industry

- Accurate Background, Inc.
- ADP Screening and Selection Services, Inc. (subsidiary of Automatic Data Processing, Inc.)
- First Advantage
- HireRight
  - Owned by Altegrity, Inc.
  - Altegrity also acquired US Investigations Services, LLC (USIS), and Kroll, Inc.
- IntelliCorp Records, Inc.
- LexisNexis
  - A Reed Elsevier Group company
  - Acquired ChoicePoint in 2008 for $4.1 billion
  - Claims to screen more individuals than any other background screening company
- Sterling Infosystems, Inc.
  - Acquired Acxiom's background screening unit, Acxiom Information Security Systems, in January 2012 and claims that it is the second largest background screening company in the world
  - Also recently acquired: Bishops Investigative Services, Abso Inc., Screening International, and Tandem Select

### *B. Local Law Enforcement's Piece of the Action*

In some cities, local law-enforcement agencies sell their own criminal background information, creating a lucrative source of revenue. A common law enforcement practice is to create a computer network for sharing information regarding bookings, arrests, and releases from county jails.[17] In Michigan, the Michigan Sheriff's Association formed a not-for-profit corporation to implement a database that stores hundreds of pieces of information about each person.[18] In 1998, the Association decided to make what it determined to be "Public Arrest Data" available to the general public. It entered into an agreement with Buckeye State Networks, LLC, which made the latter the exclusive distributor of this arrest data to private sector users.

Likewise, in the 1970s, the Onondaga County Sheriff's Department in upstate New York urged the various law enforcement agencies across the county to enter arrest information into a shared database called CHAIRS (Criminal History Arrest Incident Reporting System).[19] CHAIRS later decided to sell the information in the database for a $10 fee to employers, volunteer organizations, and landlords throughout Onondaga County.[20]

The Sheriff's Office in Monroe County, New York, took a different approach. A local trade association agreed to pay $80,000 per year to fund one full time clerk in the Sheriff's office to pull criminal records for the association.[21]

A major problem is that there are significant problems in local law enforcement records. According to a report by the Center for Community Alternatives in Syracuse, NY, a CHAIRS report is not an official criminal history report; rather, it simply is a list of all of a person's arrests in Onondaga County. The report does not include any information about whether or not these arrests resulted in a criminal conviction, a non-criminal conviction, or a dismissal.[22] The Center for Community Alternatives found that, in a review of seventy reports generated between August 2008 and April 2010, 64.3 percent of the CHAIRS reports reviewed contained at least one arrest that should not have been publicly disclosed under New York's Criminal Procedure Law. [23] Despite this disclosure of legally undisclosable information, Onondaga County Sheriff Kevin Walsh has defended the sale of these reports. Sheriff Walsh argues that CHAIRS reports provide a benefit because they are much cheaper than the $125 fee charged by the state Division of Criminal Justice Services, or the $65 fee charged by the state's Office of Court Administration.[24]

### *C. The Internet Frontier*

The Internet has facilitated the emergence of scores of online background screening companies, with many claiming instant access to millions of databases.[25] As SEARCH, a nonprofit membership organization comprised of criminal justice repositories from each of the fifty states, stated:

> When coupled with the automation of criminal justice records and the increasing power and decreasing cost of computers, the Internet creates the potential for small vendors, who would otherwise be unable to hurdle barriers to entry or, at most, would be only local players, instead to become national information providers.[26]

In fact, these online vendors have become major players in the background check business. Stephen JohnsonGrove, Deputy Director for Policy at Ohio Justice & Policy Center—a non-profit law office that seeks statewide reform of the criminal justice system—rated **backgroundchecks.com** as one of the top three background checking companies he sees.[27] On its website, **backgroundchecks.com** claims that "[w]ith a database of over 345 million criminal records" it "has now become the leader in the acquisition of data from across the country and the delivery of instant online access to public records."[28]

This growth in online vendors has occurred despite widespread public sentiment about the privacy of criminal records information. A 2000 survey by Bureau Justice Statistics that found that most adults (ninety percent) and eighty percent of young adults say that they "prefer that State agencies not use the Internet to post criminal history information that is already a matter of public record."[29] The increasing accessibility of criminal history records on the Internet also compounds the already rampant discrimination against persons with criminal records.[30] It exacerbates the disparate impact against minorities and recidivism caused by lack of employment.

### The Fair Credit Reporting Act (FCRA)

Enacted in 1970 by the U.S. Congress, the FCRA has the goal of protecting the privacy of consumers and ensuring that information is as accurate as possible. The FCRA's regulatory structure attempts to achieve those goals by imposing duties and requirements on three categories of entities:

(1) Consumer reporting agencies (CRAs): those that gather and issue consumer reports;

(2) Furnishers: those that provide information to consumer reporting agencies; and

(3) Users: those who obtain these reports and use them.

### *D. Increased Access to Public Data*

The explosion of background screening agencies, big and small, is largely due to easier access to public data. Over the past decade, criminal records have become available and used for non-law enforcement purposes to an unprecedented extent.[31] Records are made available to the public (including background screening agencies) through a variety of sources: state criminal record "central repositories" (often maintained by the State Police), the courts, private vendors which prepare reports from public sources, and even correctional institutions and police blotters (the daily written record of events in a police station often published in local newspapers).[32]

In the past, background screeners would send "runners" to the courts to manually review criminal history information. With recent technological advances, court clerks are now able to increase that accessibility by maintaining and disseminating court documents in an electronic format.[33] Today it is much more common for background screening companies to purchase large quantities of data electronically from the court or state and to populate their own databases with it.

## III. CONSUMER RIGHTS UNDER THE FAIR CREDIT REPORTING ACT

Generally, the use and dissemination of criminal background checks are regulated by the federal Fair Credit Reporting Act (FCRA) and, to a lesser extent, state fair credit reporting acts.[34] Although the FCRA is generally thought to apply to traditional credit history reports, the provisions of the Act also apply to the use and dissemination of any "consumer report," which includes criminal history records issued by commercial databases and used for employment purposes.[35]

### A. Duties of Background Screening Companies as CRAs

As with all consumer reporting agencies (CRA), background checking agencies are required to maintain procedures to ensure the accuracy of information they report about consumers. Though the law does not require reports to be free of any possible inaccuracy, it does require a CRA to have "reasonable" procedures to ensure "maximum possible accuracy."[36] Most courts consider a consumer report to be inaccurate when it is "misleading in such a way and to such an extent that it can be expected to [have an] adverse [effect]."[37]

When consumer reports are used for employment screening, the CRA has additional duties. When reporting potentially negative public record information to an employer, the CRA must do either one of two things:

- At the time that it provides the information to its customers, send the consumer a notice with the following information:
  - that the CRA is reporting criminal record information; and
  - who the report is being sent to (including name and address); or
- Maintain "strict procedures" designed to ensure that criminal record information is complete and up to date.[38]

Many background screening companies choose the option of sending a notice to the applicant to avoid the need for strict procedures.[39] However, a significant number do not, or do not provide it contemporaneously with the employer's report. To date, no court has determined exactly what "strict procedures" entail. However, as one federal district court in Pennsylvania has stated, "Without an extensive analysis of what constitutes 'strict' as opposed to 'reasonable' procedures, it stands to reason that 'strict' is necessarily a more stringent standard."[40]

With respect to the requirement for "reasonable procedures," courts generally conduct a balancing test, weighing the potential harm from inaccuracy against the burden of safeguarding such accuracy.[41] Where the potential harm is great and the burden small, a CRA's duty to prevent inaccurate or incomplete information is at its greatest.[42]

Courts have generally permitted background screening agencies to assume that court records are correct.[43] However, they do not have blanket immunity to rely on court records. For example, in one case where the CRA reported criminal background information on the wrong person, the court determined that reliance on court records did not relieve the CRA of the duty to correctly determine which public records belong to which individual consumers.[44]

Under the FCRA, a consumer has a right to request a copy of his or her consumer report and to dispute any inaccurate information.[45] Courts generally hold CRAs to a less stringent standard of accuracy when the consumer has not yet submitted a dispute. As one court stated, "[t]he consumer is in a better position than the credit reporting agency to detect errors appearing in the court documents dealing with the consumer's own prior litigation history."[46] However, in the court cases that articulate this relaxed standard of accuracy, the credit reporting agency is usually one of the "Big Three" (Experian, Equifax and TransUnion).

Relying on consumers to detect errors may be rational in traditional credit reporting, but it does not work in the criminal background context. **There are too many criminal background checking agencies for a consumer to regularly order his or her own reports to review them for errors.** Unlike the "Big Three" credit bureaus, there is no central source to find and request a copy of the report. And, even if a consumer were to try, few criminal background checking agencies have any advertised mechanism for consumers to get a copy of their own background check.[47]

There are too many criminal background checking agencies for a consumer to regularly order his or her own reports to review them for errors. Unlike the "Big Three" credit bureaus, there is no central source to find and request a copy of the report.

### *B. Duties of Employers Using Criminal Background Checks*

The FCRA also imposes duties on employers who use consumer reports to determine eligibility for employment.[48] Employers must give a series of notices if they reject an applicant based upon any information found in a background check.

First, the employer must clearly and conspicuously disclose to the applicant or employee that it will be requesting a consumer report and must obtain the employee's consent in writing to the release, and it must certify to the CRA that it has done so, and that it will make certain disclosures if adverse action is taken based in any part on the report.[49]

Second, before rejecting a candidate an employer must:

> Give the candidate a "pre-adverse action" notice including:
>
> i. A copy of the actual background check; and
>
> ii. A copy of "A Summary of Your Rights Under the Fair Credit Reporting Act".[50]

If an employer does reject a candidate based (in whole or in part) on a background check, it must then provide the candidate with an "adverse action" notice that includes:

- The name, address, and phone number of the background checking agency that supplied the report;
- A statement that the background checking agency that supplied the report did not make the decision to take the adverse action and cannot give specific reasons for it; and
- A notice of the individual's right to dispute the accuracy or completeness of any information the agency furnished, and his or her right to an additional free consumer report from the agency upon request within sixty days.[51]

### *C. Inadequacies in Employer Compliance with the FCRA*

The use of criminal background reports in employment causes unique consumer protection issues. While the remainder of this article deals with inaccuracies by consumer reporting agencies, it is worth noting that the first breakdown of consumer protection laws often occurs because many employers fail to comply with notice requirements.[52]

A user's failure to comply with notice requirements creates a "catch-22." The purpose of the FCRA notices is to ensure that the individual who is the subject has the opportunity to learn why he or she was denied employment (or adversely affected), has the opportunity to correct any errors before a decision is made, and has knowledge of his or her rights. When employers fail to comply, those seeking employment have no way of knowing that their rights have been violated, so they may never seek to enforce those rights.[53]

Even when employers do give potential employees the required pre-adverse action notice, they often fail to give the applicant adequate time to dispute any mistakes. According to the Federal Trade Commission (FTC) Staff Summary released in July 2011, there is no specific period of time an employer must wait after providing a pre-adverse action notice before taking adverse action against the consumer.[54] A prior FTC Staff Opinion had deemed five days to be reasonable, but the minimum length will vary depending on the particular circumstances involved.[55] The FTC staff author noted that the "purpose of the provisions [are] to allow consumers to discuss the report with employers before adverse action is taken."[56]

Advocates that work in the reentry community report that, on average, it takes at least two weeks to correct a consumer report and some indicate that it takes over a month.[57] This indicates that the time that the FTC had suggested prior to 2011 was inadequate to protect potential employees' rights. But the new Staff Summary may encourage or even embolden employers to allow even less time.

In fact, at least some employers are well aware of the fact that a job applicant cannot reasonably correct his or her report in the time allotted. In an email exchange, a Colgate employee stated, "The process for [the applicant] will to go back to the county court who reported conviction and prove to them that it was not him. Sterling was not able to estimate how long this would take because it really depends on the court. We are only legally required to wait 5 business days."[58]

The reality is that the FCRA, as currently interpreted, fails to adequately protect consumers when it comes to employment screening. Even applicants who successfully remove errors from their background check reports are frequently denied employment. In fact, when surveyed, several advocates indicated that they had never seen applicants get the job after correcting the report.[59] The reporting of sealed/expunged record is especially problematic for job applicants, because even if they can get a report corrected in time, there is little that can be done to "unring the bell."

Employment is unlike a denial of credit, where a consumer can simply apply for another loan or credit card if wrongly denied based upon a credit report. A denial based upon a faulty criminal background check means the denial of a potential livelihood. Jobs are scarce and new opportunities for employment do not come along that often. With a person's source of income on the line, and evidence that employer compliance with federal protections is spotty at best, it is essential that criminal background screeners do everything they can to ensure the information they give employers is accurate.

## IV. LACK OF ACCURACY IN BACKGROUND CHECK REPORTS

Despite the importance of the accuracy of criminal background report, evidence indicates that professional background screening companies routinely make mistakes with grave consequences for job seekers. Advocates from across the country report that they repeatedly see reports that:

- Contain information about a different person (i.e., a "mismatch" or false positive);
- Report sealed or expunged records;
- Are incomplete (i.e., omit disposition data);
- Display data in a way that is misleading (i.e., report a single charge multiple times); and/or
- Misclassify the type of offense.[60]

This section will discuss each of these types of errors and the ways that these errors can be avoided.

### *A. Mismatched Reports*

A very common problem with criminal background reports is false positive matches or mismatched identifications. Mismatched reports contain the criminal history of a person other than the subject of the report, due in large part to unsophisticated matching criteria.

**PublicData.com**

- Internet-based background screening company
- Searches *either* a subject's name *or* date of birth to compile matching criminal history records
- "Will NOT modify records in any database upon notification of inaccuracies."

With state-maintained databases, a biometric identification system, such as fingerprint data, is typically utilized to match a person to a record.[61] Biometric identification significantly reduces the chances of incorrectly connecting someone to the criminal record of another. In contrast, private criminal history background check companies typically match information in their databases using non-biometric information, such as name and date of birth. Moreover, due to privacy concerns, many courts will not release Social Security numbers. Therefore, many private background screening companies rely solely on first name, last name, and date of birth.

For obvious reasons, this practice poses significant trouble for people with common names. Consider the misfortunes of Catherine Taylor, an Arkansas woman with no criminal history. On several occasions, Catherine Taylor has had her housing and employment threatened because of mismatched background checks. On one occasion, the mismatched report was generated by **PublicData.com**. According to its website, **PublicData.com** is a public records disseminator.[62] It is an Internet-based background

## The Case of Catherine Taylor, Arkansas: Mismatched Report

Ms. Taylor has no criminal history, but on several occasions she has had her housing and employment threatened because of mismatched background checks.

Company: ChoicePoint (now LexisNexis)

ChoicePoint allegedly reported the criminal record of another Catherine Taylor with the same date of birth. That Catherine Taylor lived in Illinois. According to Ms. Taylor's complaint, ChoicePoint had access to other identifying information which would have distinguished these two women; however, the particular ChoicePoint product in this case was designed to give an instant result, and thus was not designed to access that information.

ChoicePoint acknowledged that next time the company generates a report on the Arkansas Catherine Taylor, the same thing will happen again.

screening company in which the user can enter *either* a subject's name *or* date of birth to compile matching criminal history records.[63]

**PublicData.com** vehemently denies being a consumer reporting agency, and attempts to disclaim any responsible for any inaccuracies in its database. However, company owner Dale Bruce Stringfellow admitted in a deposition that "they bought databases or quantities of information from governmental agencies who would be presumably clerks of court—criminal record divisions of clerk of court, and they have made that information available to [PublicData's] subscribers."[64] The fact that these reports were used for employment or other FCRA purposes should make **PublicData.com** a consumer reporting agency under the Act.

**PublicData.com** also refuses to comply with the FCRA's dispute requirements, admitting that it "will NOT modify records in any database upon notification of inaccuracies."[65] Therefore, even if Ms. Taylor alerted **PublicData.com** to its error, the company would do nothing to correct her records. Nor does **PublicData.com** do anything as simple as cross-referencing the name with the date of birth.

Even where name and date of birth do match, errors still occur. On another occasion in which Ms. Taylor was allegedly denied employment based upon an erroneous criminal background check, the company that ran the report was ChoicePoint (now LexisNexis). Ms. Taylor has the misfortune of sharing the same last name and date of birth with another Catherine Taylor, a woman living in Illinois with a lengthy criminal history.

ChoicePoint Representative Teresa Preg acknowledged that: "If an in-person court search was conducted at that time and [the court] files were pulled," ChoicePoint would have been able to determine that the two women were not "the same subject."[66] However, an in-person court search was not used in this case. Rather ChoicePoint relied on bulk data dissemination to populate its database. According to ChoicePoint, the majority of state repositories will not release social security numbers. Thus, according to the ChoicePoint representative, nothing can be done to prevent this particular problem with this particular product.

In Ms. Taylor's case, ChoicePoint had additional information—such as her address, Social Security number, and credit report—which would have indicated that she was not the person in Illinois with the criminal record. Despite the fact that ChoicePoint had access to this information, the particular ChoicePoint product in this case was designed to give an instant result, and thus *was not designed to access that information*.[67]

> *"If an in-person court search was conducted at that time and [the court] files were pulled," ChoicePoint would have been able to determine that the two women were not "the same subject."*
>
> —Teresa Preg, ChoicePoint representative (deposition)

Furthermore, ChoicePoint acknowledged that next time the company generates a report on the Arkansas Catherine Taylor, the same thing will happen, i.e., a report generated from this particular ChoicePoint product will include the information on the Illinois Catherine Taylor, even though ChoicePoint is aware of the problem. In fact, ChoicePoint claims that it cannot alter the data provided by the state repository. Therefore, even though ChoicePoint knows that the person with Arkansas Catherine's address and Social Security number is not the person with the Illinois criminal record, ChoicePoint has no mechanism to prevent the two records from merging.

Despite the acknowledged mismatch, the ChoicePoint representative said that it was "reasonable for [the potential employer] to rely on the information that is matching the information they provided us."[68] Incredibly, the representative stood by ChoicePoint's report, stating that it was reasonable to report the Illinois woman's history as the Arkansas woman's history because "of the interactive matching criteria of the first and last name and the potential that this individual was in fact the same subject."[69]

ChoicePoint is not alone in utilizing scant information to generate matches even where additional information is available. In a case in Illinois, a man named Samuel M. Jackson was allegedly denied employment after the employer requested a background check by InfoTrack Information Services, Inc. (InfoTrack), an employment screening company headquartered in Chicago, Illinois. In that case, the employer provided InfoTrack with Mr. Jackson's name and date of birth.[70] According to the complaint, the background check report that InfoTrack submitted to the employer allegedly contained seven "possible matches" from InfoTrack's nationwide sex offender database that "related to three different individuals."[71]

## The Case of Samuel M. Jackson, Chicago, Illinois: Mismatched Report

Company: InfoTrack

Mr. Jackson was allegedly denied employment after a prospective employer ran an InfoTrack background check. InfoTrack reported a rape conviction from 1987—when Mr. Jackson was four years old. The rape conviction actually belonged to fifty-eight-year-old male named Samuel L. Jackson from Virginia who was convicted of rape in November 18, 1987. And that Samuel Jackson was incarcerated at the time the InfoTrack report was run.

Mr. Jackson is a white man and was born in 1983. According to the complaint, InfoTrack had Mr. Jackson's date of birth, yet it reported information for three people, none of whom shared that same date of birth. The complaint further alleged, "three of the 'possible matches' were for a fifty-eight-year-old African American male named Samuel L. Jackson from Virginia who was convicted of rape in November 18, 1987. Plaintiff was not yet 4 years old at the time."[72] InfoTrack admitted to reporting information relating to a Samuel L. Jackson, but it denied knowing the other characteristics.[73]

However, although the exact source of InfoTrack's information is not stated in the court documents, the U.S. Department of Justice has a national sex-offender registry database through its website. A name search of this website provides not only name and location, but also, race, date of birth, height, race, date of offense, and in many cases, a picture of the offender.[74] In this specific case of Mr. Jackson, the DOJ database also indicates that the person InfoTrack listed as a possible match is presently incarcerated in Virginia—and thus unlikely to be applying for jobs in Illinois.[75]

As described in section III.A, *supra*, a consumer reporting agency that provides employers with negative public records information must either notify the consumer or follow strict procedures to ensure information is complete and up to date. InfoTrack admitted that it did not provide Mr. Jackson with a notice prior to submitting the report to the potential employer, but denied that it failed to follow strict procedures to ensure the completeness and accuracy of the report.[76] Despite this assertion that it follows strict procedures, InfoTrack's own website provides the following warning for records found using its Nationwide Criminal Database Search/Nationwide Sex Offender Registry Database Search:

> To ensure FCRA compliance, records found must be re-verified. Database searches are inherently incomplete and are to be used in conjunction with county level criminal searches.[77]

Even though it denied any wrongdoing in that case, court records show that InfoTrack settled the case with Mr. Jackson for $35,000.[78]

Mismatching people based upon a name-only match is an unbelievably common occurrence across background screening agencies. Some of the problems are attributed to a lack of available identifying information. For example, many jurisdictions will not provide background screening agencies with full Social Security numbers. Given these challenges, it is reasonable to expect that background screening companies will take measures to go beyond the face of the records to determine whether they are reporting information about the correct person. Such measures do exist. As Ms. Preg of ChoicePoint stated: "If an in-person court search was conducted at that time and [the court] files were pulled," the mistake would not have happened. Companies could also make better use of other available matching data, such as race, gender, height, and incarceration status.

Additional measures are especially necessary where the subjects of the reports have common first and last names. The frequency of names is widely available through the Census Bureau's website, and a simple algorithm could be developed to flag people who are likely to have first and last name matches with other people.[79] In fact, such algorithms already exist. A search the website, **howmanyofme.com**, estimated that there was one "Persis Yu" in the country, but approximately 45,198 "John Smith"s, 1,557 "Catherine Taylor"s, and 1,185 "Samuel Jackson"s. Therefore, while a first and last name search may be sufficient for someone with this author's name, a first and last name search will never be sufficient for a John Smith or Catherine Taylor.

Even more troubling is that background check companies have the necessary information to make a better match, but they do not design their products to utilize this information. As the deposition of ChoicePoint's Teresa Preg indicates, these companies appear to consider making information available instantly for employers and/or utilizing less costly methods to be a higher priority than ensuring accurate information for the workers whose livelihoods are affected.

## *B. Sub-sub-sub Contracting*

Another common practice in the background screening industry is to subcontract out the search for criminal records. However, the subcontracting does not stop with one vendor, but continues as the vendors themselves subcontract the work to other vendors.

As the court described in Christensen v. Acxiom Info. Sec. Sys., Inc. (Axciom):

> The erroneous information in question was acquired via a chain of requests. Mount Mercy requested information from Per Mar; Per Mar requested information from Acxiom; Acxiom requested information from a subcontractor named Ramona Batts ("Batts"); and Batts either requested information from an unidentified person then in her employ, or called the courthouse to obtain information over the telephone (Batts is not sure which way she handled this search, because she has no documentation and cannot recall the name of the employee, but she is sure that she did not go in person to the Uvalde County courthouse to handle the search in person).[80]

This practice of sub-sub-sub contracting reduces accountability and increases the likelihood of erroneous information. Moreover, background check agencies exercise scant quality control over the information provided by vendors. For example, the Per Mar representative testified that when Per Mar receives requests for consumer reports, the searches are parceled out to various vendors, but that Per Mar does not check the reports submitted by these vendors for accuracy. Instead, Per Mar relies on its vendors for accuracy.[81]

Likewise, Curt Schwall, Compliance Unit Leader at Acxiom, testified that Acxiom does not make a regular practice of checking the accuracy of negative criminal information reported by its subcontractors. When Acxiom received the information in question from Batts, an Acxiom employee typed up the consumer report. Another employee reviewed the report for compliance with the FCRA and state law. Most importantly, however, no one from Acxiom checked the accuracy of the information supplied by Batts.[82]

Acxiom's supervision and training of its subcontractors is similarly limited. Schwall testified that subcontractors such as Batts are required "to sign off on our training literature, sign a searcher agreement, and undergo quality testing." However, there was no indication that subcontractors were actually required to take a training class or undergo a training program. The quality testing consisted of periodic audits, but Schwall could not recall any of those audits. Schwall also testified that Acxiom also ran a background check on Batts.[83]

Batts testified that she was sure that Acxiom provided her some training related to the FCRA, but she could not recall its substance. Batts did not go to Acxiom's facilities for any training, nor was she provided with any videotaped training. Acxiom did not provide Batts with any information about how to read the public record. Acxiom's retainer agreement and "public record searcher contract" with Batts contain no information about compliance with the FCRA. Batts was not given any directives about reinvestigation of contested information. Batts does believe that her searches were audited by Acxiom, because she received several "certifications of excellence" from the company.[84]

Batts testified that Acxiom was "desperate for researchers," and that she agreed to do research in Uvalde County even though "it was too far" away. She also testified that she handled a large volume for Acxiom, at one time doing "doing 50 to 100 names a day," with Acxiom wanting results within twenty-four hours.[85]

Because of the vast number of public record sources in different jurisdictions that some background checking companies rely upon, it is not inherently unreasonable for them to use vendors. However, the background checking company must take responsibility to ensure that its vendors are adequately trained, supervised, audited and the information submitted by vendors must be reviewed for accuracy. Furthermore, having multiple layers of subcontracting is problematic because the practice makes it nearly impossible for any one agency to be accountable for the accuracy of the information.

### *C. Reporting Sealed or Expunged Records*

Revealing sealed or expunged data is one of the most damaging mistakes that a background checking agency can make. Unlike some other types of errors, revealing a sealed

or expunged record is nearly impossible to dispute with the employer. If the agency has mixed the job applicant's file with another person, the applicant can argue it was not him; if the applicant was ultimately exonerated, she can assert that he or she was innocent. But in the case of a sealed conviction, the applicant cannot claim that the accusation is false, but merely that the employer should not know about it. It is impossible at that point to "unring the bell."

In most states, people accused or convicted of crimes have the legal right to seal or expunge their criminal records under certain circumstances.[86] This means that the records will either be destroyed or removed from public access. Although every state has different laws and procedures for sealing or expunging records, most states will seal some records related to juvenile offenses. Many states will also seal or expunge arrest or conviction records for minor crimes like possessing marijuana, shoplifting, or disorderly conduct after a certain amount of time.[87] Sealing or expunging records is intended to give people a fresh start. When background checking agencies reveal sealed or expunged information, they deprive a job applicant to their legal right to a second chance.

One main reason these errors occur is because many consumer reporting agencies obtain their data in bulk and do not or cannot update it.

### What's the Matter with Bulk Data?

Bulk data dissemination is the practice in which public sources, often the courts, sell their data on a wholesale basis to the consumer reporting agencies. The problem arises when background screening agencies fail to update these records properly.

#### *1. Bulk Dissemination of Records*

Bulk data dissemination is the practice in which public sources, often the courts, sell their data on a wholesale basis to the consumer reporting agencies.[88] The problem arises when background screening agencies fail to update these records properly.

It is impossible to know how many expunged or sealed records are contained in the databases of consumer reporting agencies. However, a small sampling by one media outlet indicates the incidence could be significant. In June 2011, the *Salt Lake City Tribune* requested the reports of thirty people with expunged records from LexisNexis. The *Tribune* found that five out of thirty people still had criminal records that appeared on LexisNexis.[89]

A few court officials have recognized the problems created by bulk dissemination, and dissented against the practice. Tom Wilder, district clerk for Tarrant County, Texas, says expunged records are one reason he refuses to sell his county's public records to database companies in bulk.[90]

North Carolina also stopped selling its criminal records in bulk, hoping to eliminate the sloppy record-keeping practices among background screening companies.[91] Unfortunately, Mr. Wilder and North Carolina are among the minority, as most counties and states do sell public data in bulk.

Legal cases show the potential harm created by the failure to update information. For example, according to his complaint filed in court, in March 2007, Herbert VanStephens was offered a position as a store manager, conditioned on the results of a criminal background check.[92] The background check report issued by ChoicePoint indicated that in December 2002, a Cook County judge sentenced Mr. VanStephens to court supervision on a criminal charge of felony theft.[93] However in September 2006, Mr. VanStephens's criminal records were expunged from the Cook County Criminal Court database.[94]

ChoicePoint reported Mr. VanStephens's expunged record in April 2007, nearly seven months after it had been expunged from the Cook County database. According to ChoicePoint's contract with Cook County, Illinois, as well as the Cook Count Bulk Data Dissemination Policy, consumer reporting agencies are required to ensure that "all court record data will be updated and made current as of the date of dissemination [to third-parties]." Furthermore, "[t]he term, made current, as used herein shall include, but is not limited to, disseminating only court record data that is in full compliance with all statutes, court rules, and court orders (e.g. those pertaining to sealing, impounding, and expunging of court records)."[95] ChoicePoint receives information from Cook County on a weekly basis.[96] Therefore, if ChoicePoint had followed the terms of its contract with Cook County, Mr. VanStephens's information would never have been revealed.

ChoicePoint is not alone in this behavior. According to a federal lawsuit filed in Northern Illinois, in one November 2007 report issued by U.S. Commercial Services, Inc. (USIS), now HireRight, that company reported that some of its data dated from as far back as 2002, even though USIS had last updated its records in September 2007.[97] According to copies of the court records filed with the complaint, none of the records reported in the USIS report were publicly available on the date that the background check was completed.[98]

Failing to update bulk data is a systematic problem with both civil and criminal records. From approximately 2007 until 2010, Equifax failed to purchase data about satisfied, vacated, or appealed civil judgments in the state of Virginia from its vendor, LexisNexis.[99] Sometime after 2006, Equifax and its vendors stopped the more careful process of in-person manual reviews of civil courthouse records, and began collection of judgment information solely from automated resources when the Supreme Court of Virginia began providing bulk dissemination of data using electronic media.

Under the terms of the contract between LexisNexis and Equifax, LexisNexis was obligated to collect and report the existence of judgments. However, it only was obligated to collect information about the disposition of judgments if LexisNexis determined that it was "commercially reasonable" to do so. According to the complaint in the class action suit filed against Equifax and LexisNexis, LexisNexis never concluded that it was commercially reasonable to collect and report dispositions of judgments.[100]

Furthermore, when LexisNexis did receive a large batch of termination records, Equifax refused to purchase them because the purchase price exceeded the amount Equifax had budgeted for that purpose.[101]

The failure of consumer reporting agencies to purchase updated data is not limited to Virginia. In 2005, Tena Mange, spokeswoman for the Texas Department of Public Safety, which serves as a repository for public records from around the state, said the department refreshed its data daily—hourly in the case of sex offenders—but that ChoicePoint bought the data only once a month.[102] According to the district clerk for Tarrant County, Texas "[e]ven if [the background screening agencies] update weekly, their information is going to be out-of-date and a background check may not reflect what happened in the case. . . . It's not fair to the individual who has a right to get something off their record."[103] Unfortunately, many expunged cases are reported for a much longer period of time than a few days or weeks.

### 2. *State Regulation of Bulk Dissemination*

How to manage disseminated criminal records is an issue that many states have struggled with in the past decade.[104] Some state legislatures prohibit courts from disseminating their records in bulk (e.g., Idaho, Kansas, Nebraska, South Dakota, and Washington).[105] Some states take a more nuanced approach. In Arkansas, the requestor must agree, under the penalty of perjury, not to sell the bulk or compiled court records[106] and may only use the requested documents for scholarly, journalistic, political, governmental, research, evaluation or statistical purposes, in which the identification of specific individuals is ancillary to the purpose of the inquiry."[107]

In Arizona, there are two types of dissemination agreements: one for court records that include "protected personal identifiers" and one for those that do not include these identifiers.[108] Bulk court records with the personal identifiers require far more protective measures than if the requestor requested bulk data without that information. Background checking companies that purchase data with the "protected personal identifiers"—home address, exact birth date, driver's license number, and last four numbers of a social security number—must undergo periodic audits and correct sealed or corrected data within two days.[109]

This dual system has the perverse potential to encourage background screening agencies to request less information, which would then adversely affect their ability to maximize matching ability. Background screening agencies that purchase records without protected personal identifiers avoid both audits and the rules regarding correcting sealed and otherwise restricted information. At the same time this system provides a disincentive for background screeners to purchase the data that would allow them to best match the records with the subject of the background check.

North Carolina is currently one of the few states actively enforcing accuracy standards. According to an Associated Press report, "[s]tate officials say some companies paid $5,105 for the database but refused to pay a mandatory $370 monthly fee for daily updates to the files—or they would pay the fee but fail to run the update."[110] North Carolina officials also discovered that some background check companies refused to fix errors pointed out by the state or to update stale information. As a result, North Carolina revoked the licenses of CoreLogic SafeRent, Thomson West, CourtTrax, and five others for repeatedly disseminating bad information or failing to download updates.[111]

State laws on the dissemination of court records currently vary, but states have the opportunity to enact laws which could restrict the dissemination of some data or impose requirements on the background screening companies (and others) that purchase the data. However, it is also important to note that states must also have adequate resources to enforce these policies.

### *D. Incomplete Dispositions*

Another common mistake by background check companies is to omit final disposition data, that is, the companies report the fact that charges were filed, but not whether the person was convicted. Because of this omission, people who have been exonerated of the charges against, or had the charges dropped or reduced, appear to have pending criminal complaints against them.

The reporting of the disposition of pending charges can be very important to the person against whom the charges were brought. Even in cases where there has been a conviction, often the conviction will be for fewer than all of the original charges. Overcharging is a common practice, and more serious charges are often dropped as part of a plea bargain. Disposition reporting is even more important to an individual against whom all charges were dropped. Moreover, employers are reluctant to hire a worker with an ongoing legal problem. In fact, even in states that restrict consideration of criminal records for employment purposes, employers are typically allowed to deny employment to people with pending charges.[112]

As with sealed and expunged information, background screening companies fail to report the final disposition of a case because they fail to update their data. For example, people who had pending charges when the background screening company obtained its bulk data may appear to have pending charges indefinitely. This problem also occurs because background screening companies rely on sources that are known to have poor accuracy.

Under the FTC's interpretation of the FCRA, unless they provide contemporary notice to the consumer, background screening companies that furnish reports based on previously acquired public record information (purchased periodically from a third party) must verify that any such information is complete and up to date.[113]

Unfortunately, government-operated repositories are often known to have poor accuracy rates. In the 1970s, the U.S. Department of Justice ("DOJ") implemented regulations establishing minimum criteria for the handling of criminal history information by federally funded state and local criminal justice agencies.[114] These regulations led to virtually all states passing legislation governing the dissemination of criminal records to some extent.[115]

In 2006, the U.S. Attorney General reported that only half of the records in the Interstate Identification Index (III or "Triple I") system, which contains the records from all of the states and territories, included a final disposition.[116] Failure to include a disposition means that countless individuals who were ultimately acquitted or obtained dismissal of criminal charges, and whose records were sealed by the courts, could be reported as having arrests against them in perpetuity.

The state repository systems fare only nominally better. A 2008 study found that only thirty-three states reported that more than sixty percent of arrests in their criminal history databases include recorded final dispositions.[117] Twenty-three states, Guam, and the Virgin Islands reported having a backlog for entering disposition data into the criminal history database. Twenty states have reported a total of more than 1.6 million unprocessed or partially processed court disposition forms, ranging from fifty-two in Illinois to 724,541 in Utah.[118]

With respect to the dissemination of records from the central repository, these state laws vary widely, from "open record" states in which records are readily available, to "closed record" states in which dissemination is closely regulated.[119] In contrast, there has been a historical presumption of open access to court records.[120] While commercial vendors may prepare criminal record reports from any publically available source, their primary source of information is the courts, because court records usually do not share the central repositories' limitations on the availability of criminal record information.[121]

However, instead of approaching courts directly, background screening companies rely upon state court administrations which are not the keeper of the official court records. For example, in a case filed against ADP Screening and Selection Services, Inc. (ADP) in New York State, the plaintiff claimed that, in late 2008, a job offer had been rescinded because an ADP background check wrongly showed a pending arrest from 2006.[122] According to the complaint, that arrest, which was more than two years old at the time, was not pending. In fact, the plaintiff claimed that all references to the arrest had been sealed by the court in February 2008, some six months before she applied for the position.[123]

A review of the background report filed with the complaint shows that the record originated with a local county court.[124] However, the report also shows that ADP received this record from the New York State Office of Court Administration. As previously noted, background check agencies have the option of either providing a notice to the consumer that public records information was being reported for employment purposes, or to follow strict procedures to ensure that the records were complete and up-to-date. In its answer, ADP admitted that it did not provide a notice;[125] therefore, ADP was required to follow strict procedures.

From the ADP report, it appears that ADP verified the record near the date that it reported the information to the potential employer. However, ADP verified the information with the state Office of Court Administration, not with the court itself. Failure to recognize that the centralized court database is not actually the keeper of the official court records is a common mistake among background screening agencies.

In another case, the background screening company, Abso, Inc., received criminal records from the Kentucky Administrative Office of the Courts (AOC). In her affidavit to the court, Denise Best, the Kentucky Office Operations Manager for Abso, Inc. indicated that "Abso requested [plaintiff's] records from the Kentucky AOC because the Kentucky AOC is the official, and therefore, primary source repository for state-wide court records."[126] However, the Kentucky AOC does not provide official court records. In fact,

"the report generated by the Kentucky Administrative Office of the Courts indicates that it is not an official court record in bold type."[127]

Using a standard of "reasonable" rather than "strict" procedures, the court held that ABSO could rely on the information because it originated from "in Abso's experience, a presumptively reliable source" from which they had not previously received inaccurate reports.[128] Yet it is clear that court administrations are not the original source of information, because the nature of their existence is to compile information from other sources. Therefore, to ensure that final dispositions are reported, background screening companies should not report open or pending charges without additional verification directly from the court itself.

In sum, background screening companies could improve disposition reports by:

- Updating their databases;
- Selecting the most reliable sources of public information; and
- Independently seeking verification where appropriate.

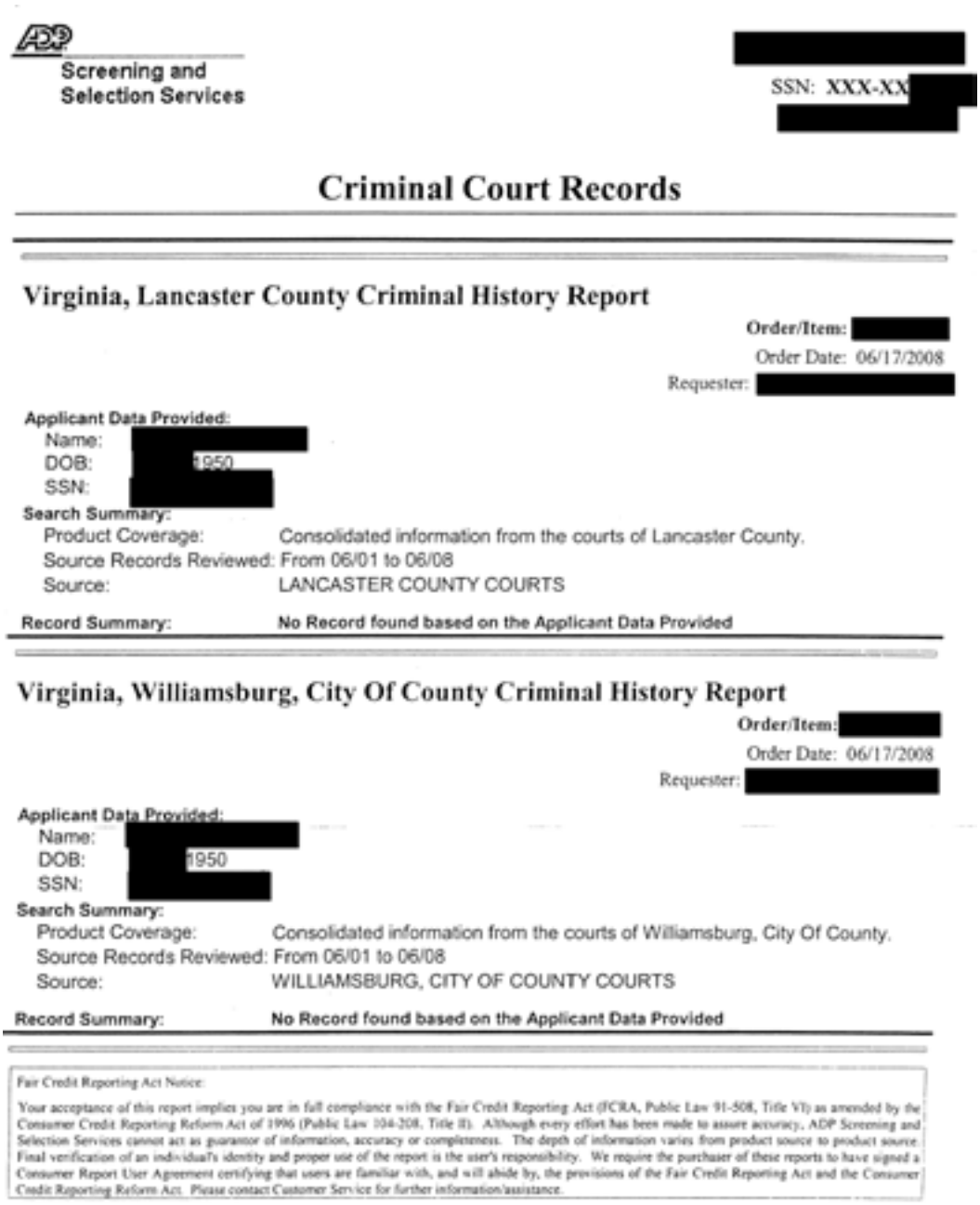
## *E. Misleading Reporting*

Another common problem is misleading reporting. Some background screening agencies dedicate considerable space on their reports to tout the jurisdictions they search, but devote significantly less space to the results of those searches.

For example, an ADP report (see redacted report on next page) on a Philadelphia resident dedicated one and a half pages to listing three different county courts in Virginia in which ADP conducted the search. In font smaller than all the other fonts in the records, the report states: "No record found based upon the Applicant Data Provided." Therefore, any employer who only gave the report a quick glance could easily think that the person *did* have a record in those jurisdictions, when in fact he did not.[129]

**Background screening agencies are also known to report single arrests or incidents multiple times**. On the same ADP report, ADP reported ten charges twice (from only two cases)—once as reported from the court's database and a second time from the Commonwealth of Pennsylvania Common Pleas Case Management System database. The ADP report was 28 pages long, yet essentially presented information about two cases. Information was provided redundantly for every single count (including birth date, gender, race, and physical description). This voluminous presentation suggested that the person had a massive rap sheet, when in fact there were only two cases.[130]

The problem of multiple reporting of a single conviction has happened repeatedly to Bahir Smith in Philadelphia, PA. Mr. Smith is a truck driver, which is an industry that subjects him to many criminal background checks. Mr. Smith only has one arrest on his criminal record. Yet according to his complaint, in March 2009, USIS issued a report comprised of nine pages and listed that single arrest three different times.[131] Nearly a year later, USIS allegedly issued another report, in which that same case was listed four times.



ADP
Screening and
Selection Services

[redacted]
SSN: XXX-XX[redacted]

## Criminal Court Records

### Virginia, Lancaster County Criminal History Report

Order/Item: [redacted]
Order Date: 06/17/2008
Requester: [redacted]

Applicant Data Provided:
Name: [redacted]
DOB: [redacted]1950
SSN: [redacted]

Search Summary:
Product Coverage: Consolidated information from the courts of Lancaster County.
Source Records Reviewed: From 06/01 to 06/08
Source: LANCASTER COUNTY COURTS

Record Summary: No Record found based on the Applicant Data Provided

### Virginia, Williamsburg, City Of County Criminal History Report

Order/Item: [redacted]
Order Date: 06/17/2008
Requester: [redacted]

Applicant Data Provided:
Name: [redacted]
DOB: [redacted]1950
SSN: [redacted]

Search Summary:
Product Coverage: Consolidated information from the courts of Williamsburg, City Of County.
Source Records Reviewed: From 06/01 to 06/08
Source: WILLIAMSBURG, CITY OF COUNTY COURTS

Record Summary: No Record found based on the Applicant Data Provided

Fair Credit Reporting Act Notice:

Your acceptance of this report implies you are in full compliance with the Fair Credit Reporting Act (FCRA, Public Law 91-508, Title VI) as amended by the Consumer Credit Reporting Reform Act of 1996 (Public Law 104-208, Title II). Although every effort has been made to assure accuracy, ADP Screening and Selection Services cannot act as guarantor of information, accuracy or completeness. The depth of information varies from product source to product source. Final verification of an individual's identity and proper use of the report is the user's responsibility. We require the purchaser of these reports to have signed a Consumer Report User Agreement certifying that users are familiar with, and will abide by, the provisions of the Fair Credit Reporting Act and the Consumer Credit Reporting Reform Act. Please contact Customer Service for further information/assistance.

The same problem, also involving USIS, happened to A. Garcia in Chicago, IL. USIS listed one case in his report three separate times. A review of the report indicates that each of those entries was the result of USIS running a search on a different date. Each entry looks slightly different. Therefore, it appears that USIS simply included what it found each time, and did not review the information to see if it matched with a record already in the report.[132]

In all of these reports, a simple review of the information would have revealed that the same case was being reported several times. At best, the duplicate reporting is the result of sloppy practices by background screening companies, such as failing to recognize the same case reported by multiple sources or by poor report formatting. At worst, it could be an example of padding to make the report appear more consequential, and persuade employers that they got their money's worth.

Another type of misleading practice occurs when background screening agencies attempt to subvert the time limits for information in the FCRA by telling potential employers that the company has information that it could not share. For example, SterlingInfo included the following paragraph in applicable background checks:

> This applicant has an arrest/incident on his/her criminal history that is NOT a conviction, and is over 7 years old. In accordance with Federal guidelines, we need to verify that this applicant will make at least $75,000 per year in order to make this information available to you. If you wish to receive this information, please let us know that the applicant meets this salary threshold by emailing **SalaryConfirmation @sterlingtesting.com**.[133]

SterlingInfo has defended this practice by claiming that "[D]efendant did not disseminate any arrest records of plaintiff in violation of 15 U.S.C. §1681(c). To the contrary, defendant merely advised its client that arrest records older than 7 years existed."[134] However, a federal district court in Pennsylvania found that the existence of adverse information was itself adverse information, and therefore, subject to the FCRA.[135]

### *F. Misclassification of the Type of Offense*

Sometimes criminal background screening agencies just get the information wrong. Every state has its own criminal justice system, and each state works differently. Advocates from across the country report that they often see mistakes on commercial background reports due to a fundamental misunderstanding of how that state reports and classifies information. Specifically, commercial background screening agencies repeatedly misreport the level or classification of the offense. Additionally, they rarely know what to do with offenses that are classified as less than a misdemeanor or are non-criminal offenses (violations of law that are not classified as crimes, such as traffic tickets).[136]

In a background check on a Pennsylvania man, Phenix Group, Inc. incorrectly reported the grade of a conviction. Although the man was charged with a felony and two other misdemeanors, those charges were dropped. Instead, he pled guilty to two "summary offenses" for public drunkenness and defiant trespass. In Pennsylvania, summary offenses are below the level of a misdemeanor and may not be used by employers in hiring decisions. Because of this mistake, when he applied for a job, his application was rejected.[137]

In New York, the Center for Community Alternatives sees background screening companies misclassify records based upon the court where the case was adjudicated. Although the bulk of the cases prosecuted in New York Superior Court are felonies, some cases originate in Superior Court as part of its "integrated domestic violence" program.

Patricia Worth, Co-Director of Justice Strategies, Center for Community Alternatives, has seen background screening companies report this type of record as a felony conviction. In one case, the original arrest was only a misdemeanor, and the conviction was for a non-criminal violation. However, despite the fact that the Penal Law code indicated that it was a non-criminal violation, the background checking agency reported the conviction as a felony. Apparently, the agency assumed that because the case was prosecuted in Superior Court, it must be a felony.[138]

## V. ATTEMPTING TO CONTRACT OR DISCLAIM AWAY FCRA DUTIES

Another disturbing trend among background checking agencies is their attempts to circumvent the Fair Credit Reporting Act through disclaimers and clever contracting.

In a deposition with Keith Alan Clifton, President of TenantTracker, which provides criminal records for the purpose of tenant screening, Clifton admits that he advises his clients that the records might not be accurate.

> **Question:** Do you—when you publish a report in response to a customer's inquiry, do you expect the customer to be able to rely upon the accuracy of that report?
>
> **Clifton:** Within the context of how I've provided the service under our contract.
>
> **Question:** Well, are you saying that there are certain qualifiers or disclaimers of accuracy in your contract?
>
> **Clifton:** Yeah.
>
> **Question:** So when you contract with your customer, you're contracting and advising your customer not to rely upon the accuracy of your report?
>
> **Clifton:** I'm advising them that they need to be a part of the process and that to ensure accuracy we have to work together.
>
> **Question:** And do you believe that such a contractual provision complies with the Fair Credit Reporting Act?
>
> **Clifton:** Yeah, I do.[139]

In the deposition, Clifton goes on to describes the process in which he instructs the user how to determine whether the subject of the report is the same person that the user is conducting the search on. In the case described above, TenantTracker had information indicating that the name and race of the individual searched did not match the subject of the report. However, TenantTracker did not fix the report until the user (its customer) indicated that the report did not seem to match the person it was seeking information about.

Dale Bruce Stringfellow, the authorized representative of **PublicData.com** (which takes the position it is not a CRA) explains the company's reporting of criminal records in this way:

> "What we've done as adults is we've looked through these listings and said, okay, well, there's a Catherine Taylor, but PublicData does not assert that the Catherine Taylor with the birth date that shows up is—is your client. And so we don't—we don't behind the scene make any—any claims such as that."[140]

Thus, according to Stringfellow, because PublicData never actually claims that the information it gives to the user pertains to the person about whom the user requested information, the company is not responsible for the accuracy of the information. [141]

This attempt to disclaim FCRA duties by contract is not limited to small-time operations. In fact, ChoicePoint (now LexisNexis), one of the largest background screening agencies, also attempts to contract away its FCRA duties. According to ChoicePoint representative Theresa Preg, depending on the service the user purchases, ChoicePoint's only duty is to give the user the information it has.

> **Preg:** [T]he product that was purchased by American Red Cross is an instant search against the criminal records database and an instant certainly [sic] of the Social Security number verification. [This] is in order to provide American Red Cross with as much information as possible and the fact that a subject may or may not have a criminal record, we would match, use our search criteria and the matching identifying information of at least the three identifiers and return that information with additional data and allow them to make any further determination with the consumer directly or through ChoicePoint if there's any question regarding the information that's provided back to them in this instant format.
>
> **Question:** Now, at the top of this report, . . . you have included a notice stating that the report does not guarantee the accuracy or truthfulness of the information; is that true?
>
> **Preg:** That is true, that's on the report.[142]

Likewise, in its advertising, InfoTrack admits that results of its Instant Sex Offender registry might be inaccurate. InfoTrack's website states: "To ensure FCRA compliance, records found must be re-verified."[143]

Unfortunately, some courts have permitted this type of legal sidestepping. These courts have held background screening companies not to be liable even though the background check provided criminal records of a different person.[144] As one court reasoned, the company provided an "accurate reporting of court records," even if the records were not attributable to the intended subject.[145] The court relied on the fact that the report warned that the list contained "possible" matches as opposed to "confirmed identical matches" and that the disclaimer sufficiently "identifie[d] the nature of the information and its limitations."[146]

There are several problems with this reasoning, which permits background screening agencies to use disclaimers to circumvent the Fair Credit Reporting Act.

First, the notion that users "need to be a part of the process and that to ensure accuracy we have to work together" is both unrealistic and harmful to the worker who is

the subject of the reports. Employers seldom read the disclaimers and believe that the report they have bought is accurate and stands on its own. The worker does not typically have a choice as to which company runs the report or which product the employers should use. The worker is at the mercy of the economic whims and demands of both the employer and the background screening agency.

Second, the consumer has no way to enforce the background check agency's requirements on the user. The "everyone works together to ensure accuracy" approach does not work if the employer does not have the desire or the expertise to live up to its end of the bargain. Though they may have some contractual duty to the background screening agency, employers have no duty to the worker that is the subject of the report—either contractually or under the FCRA.

Finally, the most egregious problem is that the accuracy of the background reports appears to be commensurate with the price of the service the employer is willing to pay. As demonstrated with PublicInfo, ChoicePoint, and InfoTrack as previously described, there is clearly a demand for instant access to criminal records. However, this instant access comes at the price of accuracy.

## VI. WHAT WOULD REASONABLE PROCEDURES LOOK LIKE?

The purpose of this report is not to argue that background screening companies are bad, but that there are serious concerns about the accuracy of their products. The National Association of Professional Background Screeners (NAPBS) has made an attempt to bring order to the Wild West of background screening companies. According to its materials, the NAPBS has established an accreditation program, the Background Screening Agency Accreditation Program (BSAAP), to advance "professionalism in the employment screening industry through the promotion of best practices, awareness of legal compliance, and development of standards that protect consumers."[147]

Background screening companies that voluntarily participate in the BSAAP agree to follow the NAPSB's Standards and to submit to an auditing process. If all background screening companies followed the NAPSB Standards, many elements of which simply require compliance with the FCRA, there would be many fewer errors on criminal background reports.

Less than one percent of background screening agencies are actually certified by NAPBS—meaning less than one percent undergo voluntary audits by their own trade association and commit themselves to comply with Standards that contain many legally mandated elements.

Although these Standards are a good start for the industry and indeed probably legally required, they certainly do not go far enough to adequately protect consumers. Many of the requirements are vague and simply reflect the language in the Fair Credit Reporting Act. Additionally the Standards merely call for the existence of procedures to deal with accuracy issues, as opposed to dictating what those procedures should be.

## Notable elements of the NAPSB Standards

1. The [consumer reporting agency] CRA shall have procedures in place for handling and documenting a consumer dispute that comply with the federal FCRA.
2. When reporting potentially adverse criminal record information derived from a non-government owned or non-government sponsored/supported database pursuant to the federal FCRA, the CRA shall either: A) verify the information directly with the venue that maintains the official record for that jurisdiction prior to reporting the adverse information to the client; or B) send notice to the consumer at the time information is reported.
3. The CRA shall designate an individual(s) or position(s) within the organization responsible for compliance with all state consumer reporting laws that pertain to the consumer reports provided by the CRA for employment purposes.
4. The CRA shall have procedures in place to inform clients that they have legal responsibilities when using consumer reports for employment purposes. The CRA shall recommend that clients consult their legal counsel regarding their specific legal responsibilities.
5. The CRA shall follow reasonable procedures to assure maximum possible accuracy when determining the identity of a consumer who is the subject of a record prior to reporting the information. The CRA shall have procedures in place to notify client of any adverse information that is reported based on a name match only.
6. The CRA shall designate a qualified individual(s) or position(s) within the organization responsible for understanding court terminology, as well as understanding the various jurisdictional court differences if the CRA reports court records.
7. Should the CRA receive information from the verification source subsequent to the delivery of the consumer report, and as a direct result of the initial inquiry, that conflicts with originally reported information, and that new information is received within 120 days of the initial report (or as may be required by law), the CRA shall have procedures in place to notify the client of such information.

Also, despite the fact they are legally required and as barebones as the NAPBS Standards are, *very few background screening companies have voluntarily become accredited under this program*. Out of the 2,137 members in its online directory, the NAPBS only lists 21 accredited companies in its directory. Thus, less than one percent of background screening agencies are actually certified by NAPBS—meaning less than one percent undergo voluntary audits by their own trade association and commit themselves to comply with Standards that contain many legally mandated elements.

In addition to the requirements in the NAPBS Standards, adopting other practices would do much more to ensure the fidelity of criminal background checks.

### *A. Avoiding Duplicate Reporting of a Single Case*

Background screening companies should develop reliable matching criteria that allow duplicate reporting of a single case to be identified and avoided. Specifically, this software should search for indications that two records are in fact the same case. Such matching criteria would include:

1. Arrest date
2. Disposition date
3. Jurisdiction—state; court and/or county
4. Convicted—yes/no
5. Number of charges
6. Offense type—felony, misdemeanor, other
7. Case number
8. Name of charges
9. Disposition
10. Sentence

In many cases, not all ten data fields will match or will be available. However, not all ten criteria should need to match in order for the background screening company to reliably determine that the cases are the same. As few as five or six criteria could be enough to establish a match.

### *B. Avoiding Mismatched Data*

Background screening companies should use all available criteria to match a consumer with a record in a criminal database. These criteria should include a combination of name, date of birth, social security number, former residences, gender, race, and physical description (such as height and weight). Although not all of these criteria will be available in every public database, background screening companies should obtain all that are available, and should match as many as possible to the subject of the report. In addition, background screening companies should view non-match of certain criteria, at a minimum, as a red flag that a record should be more extensively reviewed before concluding that there is a match.

Because not all matching criteria serve the same function, the criteria should be split into three categories as shown below.

| Level 1: Criteria that can match a specific individual. | Level 2: Criteria that can disqualify a potential match. | Level 3: Criteria that should raise a red flag. |
|---|---|---|
| • Full Name<br>• Date of Birth<br>• Full Social Security Number (all nine digits) | • Gender<br>• Race<br>• Physical Description | • Address/State does not match any former residence of the consumer<br>• Middle initial or Suffix do not match<br>• Consumer has a common name |

*A user should obtain information on all of these criteria from the consumer when seeking permission for the background check.* This will permit maximum possible accuracy in matching by the background screening companies.

*A background screening company must match either the full Social Security number or at least the two other Level One criteria plus a Level Two criterion*. Note that Social Security numbers are the only unique identifiers (and even they can be misrecorded, stolen, or falsified). There are many cases in which even a name and date of birth match will be inadequate, because of coincidence matches (especially with common names). This is particularly true in fifty-state background checks. Matching of Level Two criteria should be attempted to bolster the accuracy of a match not including a Social Security Number.

Name-only matches should never be used. Tens of thousands of people share certain common names.

*Name-only matches should never be used.* Tens of thousands of people share certain common names. A name-only match is never sufficient.

*If any Level Two criteria are available but do not match, that record should be excluded from any criminal background report*. For example, an arrest record that matches a consumer's name and date of birth, but lists a female when the consumer is a male should not be included in a criminal background report.

*If any Level Three criteria are available and do not support a match, a red flag should be raised as to the accuracy of a match between the consumer and the record*. For example, an arrest record matches the consumer's name and date of birth, but the consumer has a common name, John Smith, and has never lived in California, the source of the arrest record. In such a situation, the background screening agency should scrutinize the record and only include it if a totality of the other factors weighs towards its inclusion. This process would require human intervention, not just database matching.

### C. Ensuring that Records Are Complete and Up-to-Date, and No Sealed or Expunged Information Is Provided

Background screening companies should verify criminal record information with the *original* source of the information immediately prior to reporting it. Background screening companies should also send the consumer a notice that they intend to report the negative information *before* they send the information to the prospective employer, so that incomplete information can be addressed prior to dissemination.

Additionally, background screening companies that use stored bulk data should implement synchronization software that permits the "synching" of data so that previously reported cases that have been sealed or expunged can be identified and removed. Synching of data between two separate sources has become ubiquitous, and tens of millions of consumers regularly use software that permits a smart phone or an MP3 player to synchronize with a personal computer. Background screening companies should be required to do the same. Synching software can include "conflict detection," which permits the modification of a file to be identified.

Alternatively, background screening companies should request that their public agency sources of criminal case information produce lists of expunged cases for the companies to correct their databases. For example, in April 2010, the Administrative Office of Pennsylvania Courts (AOPC) announced that it would affirmatively produce weekly lists of expunged cases for subscribers to its bulk distributions of criminal case data. This so-called "LifeCycle File" informs subscribers of information that should be removed from a database. It contains updates for all of the courts for which AOPC provides electronic information. Information contained in the file includes the court, the docket number, the outcome, and the date. AOPC requires its bulk subscribers use this information to remove expunged cases.

Finally, all arrest data that are more than one year old and lack final disposition data should be verified with the official source of the information to see whether a final disposition has occurred.

## VII. RECOMMENDATIONS

As this report demonstrates, background screening companies frequently include inaccurate, misleading, and incorrect information on criminal history reports prepared for employment purposes. Both federal and state governments have a role to play in reigning in the "Wild West" of criminal background screening.

### *A. Federal Recommendations*

The rulemaking scheme for the FCRA was drastically altered with the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act).[148] The Dodd-Frank Act established a new agency, the Consumer Financial Protection Bureau (CFPB), and transferred the bulk of the rulemaking authority for the FCRA to the CFPB .[149] The Dodd-Frank Act also granted general rulemaking authority to the CFPB, enabling it to ''prescribe such regulations as are necessary to carry out the purposes of this title'' and ''as may be necessary or appropriate to administer and carry out the purposes and objectives of this title, and to prevent evasions thereof or to facilitate compliance therewith.''[150] This is an authority that the Federal Trade Commission, which previously enforced much of the FCRA, was never granted.

The CFPB should use its FCRA rulemaking ability to:

1. Define reasonable procedures to ensure maximum possible accuracy under Section 1681e(b) of the FCRA to include:
   a. Requiring verification and updating of criminal records that lack disposition data for records more than one year old.
   b. Requiring all consumer reporting agencies to use all available data to determine matches.
   c. Prohibiting name-only based matches.

d. Prohibiting multiple reports of the same case regardless of source.
e. Clarifying what information can be included with convictions and arrests in order to prevent concurrent charges from being treated as additional convictions.

2. Define "strict procedures" under 1681(k) to require verification of all criminal records that lack disposition data.
3. Produce guidelines on matching criteria, especially for consumers with common names.
4. Define how long an employer has to wait between sending a pre-adverse notice under 1681b(b)(3) and taking adverse action. The period should allow adequate time to correct the record, such as thirty-five days.
5. Require registration of consumer reporting agencies.

Since the FCRA was adopted in 1970, the Federal Trade Commission (FTC) has been the agency primarily responsible for interpreting the Act. While the Dodd-Frank Act shifted the authority to publish FCRA rules and guidelines to the CFPB, the FTC will retain enforcement authority over much of the background check industry under the FCRA.

The FTC should use its FCRA enforcement authority to:

1. Investigate major commercial background screening companies for common FCRA violations.
2. Investigate major, nationwide employers for compliance with FCRA requirements imposed on users of consumer reports for employment purposes.

## *B. State Recommendations*

As the source of most of the data reported by background screening agencies, states have a huge role to play in ensuring the accuracy of criminal background checks. Therefore, state legislatures, administrative agencies, or court systems should implement the following policies:

1. State repositories, counties, and other public records sources should require companies that have subscriptions to receive information by bulk dissemination from court databases to have a procedure for ensuring that sealed and expunged records are deleted.
2. State repositories, counties, and other public records sources should audit companies that purchase bulk data to ensure that they are removing sealed and expunged data. Companies that fail such audits should have their privilege to receive bulk data revoked.

## VIII. CONCLUSION

This report describes a number of ways in which background screening companies make mistakes that greatly affect a consumer's ability to find employment. Although the mistakes discussed in this report are not inclusive of all errors found on background checks, attorneys and community organizations that work with consumers with faulty background reports report that they repeatedly see background reports that:

- Mismatch the subject of the report with another person;
- Omit disposition information;
- Reveal sealed information;
- Contain misleading information; and
- Mischaracterize the seriousness of the offense reported.

Many of these errors can be attributed to common practices by background screening companies, such as:

- Retrieving information through bulk record disseminations and failing to routinely update the database;
- Failing to verify information obtained through subcontractors and other faulty sources;
- Utilizing unsophisticated matching criteria;
- Failing to utilize all available information to prevent a false positive match; and
- Lacking understanding about state specific criminal justice procedures.

As discussed, even the National Association of Professional Background Screeners agrees there are some simple procedures that background checking companies can take to enhance the quality of their information. Unfortunately, few companies actually are willing to commit to even the limited recommendations of their own trade association.

With the explosive growth of this industry, it is essential that the "Wild West" of employment screening be reined in so consumers are not guilty until proven innocent. Lack of accountability and incentives to cut corners to save money mean that consumers pay for inaccurate information with their jobs and, thus, their families' livelihood.

Criminal background checking is big business, and ensuring accurate and complete information has costs. With the explosive growth of this industry, it is essential that the "Wild West" of employment screening be reined in so consumers are not guilty until proven innocent. Lack of accountability and incentives to cut corners to save money mean that consumers pay for inaccurate information with their jobs and, thus, their families' livelihood.

# ENDNOTES


1. Bur. of Labor Statistics, U.S. Dep't of Labor, The Employment Situation—March 2012 (2012), *available at* **www.bls.gov/news.release/pdf/empsit.pdf**.
2. Soc. for Human Res. Mgmt., Background Checking: Conducting Criminal Background Checks (Jan. 22, 2010), *available at* **www.shrm.org/Research/SurveyFindings/Articles/Pages/ConductingReferenceBackgroundChecks.aspx**.
3. Michelle Natividad Rodriguez & Maurice Emsellem, The Nat'l Employment Law Project, 65 Million Need Not Apply, The Case for Reforming Criminal Background Checks for Employment (Mar. 2011). Many people who have a criminal record that shows up on a background check have never been convicted of a crime; in fact, one-third of felony arrests never lead to conviction. U.S. Bur. of Justice Statistics, Felony Defendants in Large Urban Counties, 2004 (Apr. 2008).
4. Equal Employment Opportunity Comm'n, Fact Sheet on Employment Tests and Selection Procedures, **www.eeoc.gov/policy/docs/factemployment_procedures.html** (last visited Dec. 27, 2011).
5. Rodriguez & Emsellem, *supra* note 3 at 5.
6. Christopher Uggen, *Work as a Turning Point in the Life Course of Criminals: A Duration Model of Age, Employment, and Recidivism*, 67 Am. Sociological Rev. 529 (2000).
7. Rodriguez & Emsellem, *supra* note 3 at 3.
8. *Id*. at Endnote 4. In their 2010 survey, the Society for Human Resource Management found that 55 percent of employers report using criminal background checks in order to reduce their legal liability for negligent hiring. Society for Human Resource Management, Background Checking: Conducting Criminal Background Checks (Jan. 22, 2010), *available at* **www.shrm.org/Research/SurveyFindings/Articles/Pages/ConductingReferenceBackgroundChecks.aspx**. Yet according to one study of negligent hiring claims, only 10 percent of claims filed in 2003 involved the hiring of persons with a criminal histories and only 50 percent of those plaintiffs received favorable decisions. April Frazier, Nat'l HIRE Network, Negligent Hiring: Myth or Reality for Employers (2008), *available at* **www.eastcounty1stop.org/docs/neg_hiring_1_30_08.pdf**.
9. Alfred Blumstein & Kiminori Nakamura, *'Redemption' in an Era of Widespread Criminal Background Checks*, 263 NIJ Journal 10, 12-13 (2009).
10. *See, e.g.*, Ctr. for Cmty. Alternatives, A Report to the Alliance of Communities Transforming Syracuse (ACTS): The Use of CHAIRS Reports as Criminal Background Checks (Mar. 2011), *available at* **www.communityalternatives.org/pdf/CHAIRS-FullReport-FINAL-March 2011-1.pdf**; Sharon Dietrich, Cmty. Legal Servs., Inc., Philadelphia, PA, Expanded Uses of Criminal Records and Its Impact on Re-entry (March 3, 2006); Louis Prieto, Persis Yu, & Jason Hoge, *Using Consumer Law to Combat Criminal Record Barriers to Employment and Housing Opportunity*, Clearinghouse Rev. (Jan-Feb. 2011).
11. *See generally* SEARCH, the Nat'l Consortium for Justice Info. and Statistics, Report of the National Task Force on the Commercial Sale of Criminal Justice Record Information (2005) (hereinafter National Task Force Report on Commercial Sale of Criminal Record Information) at 7, *available at* **www.search.org/about/news/2005/reports.asp**.
12. *Id.* at 4.
13. *Id*. at 32.
14. Ann Davis, *Firms Dig Deep Into Workers' Pasts Amid Post-Sept. 11 Security Anxiety*, Wall St. J (Mar. 12, 2002).

15. Reed Elsevier Press Release, *Reed Elsevier to acquire ChoicePoint, Inc.* (Feb. 2008), *available at* **www.reed-elsevier.com/mediacentre/pressreleases/2008/Pages/ReedElseviertoacquireChoicePoint,Inc.aspx**.
16. Chad Terhune, *The Trouble with Background Checks*, Bus. Wk. (May 29, 2008), *available at* **www.businessweek.com/magazine/content/08_23/b4087054129334.htm**.
17. *See, e.g.*, Lewis v. Ohio Prof'l Elec. Network L.L.C., 248 F. Supp. 2d 693, 696 (S.D. Ohio 2003); Center for Community Alternatives, *supra* note 10.
18. Lewis, 248 F. Supp. 2d at 696.
19. Center for Community Alternatives, *supra* note 10 at 3-4.
20. *Id.* at 3-4.
21. Agreement between County of Monroe, the Monroe County Sheriff, and the Foundation for Quality Care Upstate (Feb. 17, 2009) (on file with author).
22. Center for Community Alternatives, *supra* note 10 at 3.
23. *Id*. at 11.
24. The Post-Standard Editorial Board, *Stop Selling Them: Unreliable CHAIRS Reports Do More Harm Than Good*, Syracuse Post-Standard, April 14, 2011, *available at* **http://blog.syracuse.com/opinion/2011/04/stop_selling_them_unreliable_c.html**.
25. SEARCH, National Task Force Report on Commercial Sale of Criminal Record Information, *supra* note 11 at 29.
26. *Id*.
27. National Consumer Law Center, Informal Survey of National Employment Law Project's Criminal Records Listserv Members (Nov. 2011) (on file with author) (hereinafter NCLC Survey).
28. **Backgroundchecks.com**, About Us, **www.backgroundchecks.com/info.mvc/about-us** (last visited December 9, 2011).
29. Bureau of Justice Statistics, U.S. Dep't of Justice, Privacy, Technology, and Criminal Justice Information: Public Attitudes Toward Uses of Criminal History Information (July 2001) at 45.
30. Keith Finlay, Nat'l Bur. of Economic Research, Effect of Employer Access to Criminal History Data on the Labor Market Outcomes of Ex-Offenders and Non-Offenders (May 12, 2008).
31. Dietrich, *supra* note 10 at 1.
32. SEARCH, National Task Force Report on Commercial Sale of Criminal Record Information, *supra* note 11 at 29.
33. Texas Judicial Counsel, Public Access to Court Case Records in Texas: A Report with Recommendations (Aug. 2004), *available at* **www.courts.state.tx.us/tjc/pdf/final%20public%20access%20council%20report.pdf**.
34. *See generally* National Consumer Law Center, Fair Credit Reporting §§ 2.3 and 3.2.4 (7th ed. 2010 and Supp.).
35. *Id*. *See also* Prieto, et al., *supra.* note 10.
36. 15 U.S.C. § 1681e. *See also* National Consumer Law Center, Fair Credit Reporting § 4.4.5 (7th ed. 2010 and Supp.).
37. *See generally* National Consumer Law Center, Fair Credit Reporting § 4.2.3 (7th ed. 2010 and Supp.).
38. 15 U.S.C. § 1681k.
39. *See generally* National Consumer Law Center, Fair Credit Reporting § 4.4.7 (7th ed. 2010 and Supp.).
40. Smith v. HireRight Solutions, Inc., 711 F. Supp. 2d 426, 439 (E.D. Pa. 2010). *See also* National Consumer Law Center, Fair Credit Reporting § 4.4.7 (7th ed. 2010 and Supp.).
41. *See generally* National Consumer Law Center, Fair Credit Reporting § 4.4.5 (7th ed. 2010 and Supp.).

42. *Id.*
43. Henson v. CSC Credit Servs., 29 F.3d 280, 286 (7th Cir.1994) (holding that a "credit reporting agency is not liable under the FCRA for reporting inaccurate information obtained from a court's Judgment Docket, absent prior notice from the consumer that the information may be inaccurate"). *See also* Haro v. Shilo Inn, 2009 WL 2252105 (D. Or. 2009).
44. *See* Adams v. Nat'l Eng'g Serv. Corp., 620 F. Supp. 2d 319, 334 (D. Conn. 2009).
45. 15 U.S.C. §§ 1681h(a)(1), 1681j(a)(1)(A). *See generally*, National Consumer Law Center, Fair Credit Reporting §§ 3.5.1 and 8.5.4 (7th ed. 2010 and Supp.).
46. Henson, 29 F.3d at 285.
47. A search of the following websites did not reveal a way for a consumer to obtain a copy of his or her background check: Accurate Background, Inc., **www.accuratebackground.com/resources.php?sec=145**; Automatic Data Processing, Inc., **www.adp.com** (last visited Dec. 27, 2011); IntelliCorp Records, Inc., **www.intellicorp.net**.
48. 15 U.S.C. § 1681b(b)(2). *See generally*, National Consumer Law Center, Fair Credit Reporting § 7.2.4 (7th ed. 2010 and Supp.).
49. *Id.*
50. 15 U.S.C. § 1681b(b)(3).
51. 15 U.S.C. § 1681m.
52. *See, e.g.*, Williams v. Staffing Solutions Southeast, Inc., d/b/a Prologistix, No. 10-cv-00956 (N.D. Ill. Feb. 11, 2010); Liccione v. Wilson Farms, No. 09-cv-06544 (W.D.N.Y. Oct. 29, 2009).
53. Prieto et al., *supra* note 10 at 474-476.
54. Federal Trade Comm'n, 40 Years Of Experience With the Fair Credit Reporting Act: An FTC Staff Report With Summary of Interpretations (July 2011) at 52-53.
55. *Id*. This Summary effectively withdraws the prior FTC Staff Opinion stating that 5 days is reasonable.
56. Lewis, FTC Informal Staff Opinion Letter, June 11, 1998.
57. NCLC Survey, *supra* note 27.
58. Defendant's Motion for Summary Judgment, Exhibit F (e-mail from Courtney Gentile to Kandy Clark and Dorothy Gerner), Poore v. Sterling Testing Sys., Inc., 410 F. Supp. 2d 557 (E.D. Ky. 2006).
59. NCLC Survey, *supra* note 27.
60. *Id*.
61. Bur. of Justice Statistics, U.S. Dep't of Justice, Survey of State Criminal History Systems, 2008, (2008) at viii.
62. **PublicData.com**, *Frequently Asked Questions*, **www.publicdata.com/faq.htm** (last visited October 12, 2011).
63. Deposition of Dale Bruce Stringfellow, Jr. at 43, Taylor v. The Source for PublicData, LP d/b/a **PublicData.com** and IntelliCorp Records, Inc., No. 07-CV-00880 (E.D. Ark. October 23, 2008).
64. *Id*. at 72:2-8.
65. **PublicData.com**, *supra* note 62.
66. Deposition of Teresa Preg at 66:4, Taylor v. Equifax, et al, No. 4:06CV0496-GTE (E.D. Ark. Dec. 2006).
67. *Id.* at 63-64.
68. *Id.* at 62:6-9.
69. *Id.* at 62:6-18.
70. Answer at 1-2, Jackson v. InfoTrack, No. 11-cv-5801 (N.D. Ill. Sept. 16, 2011).
71. Class Action Complaint at 3, Jackson v. InfoTrack, Case No. 11-cv-5801 (N.D. Ill. Aug. 23, 2011).
72. *Id*.

73. Answer at 5, Jackson v. InfoTrack, No. 11-cv-5801 (N.D. Ill. Sept. 16, 2011).
74. The Dru Sjodin National Sex Offender Public Website, **www.nsopw.gov** (last visited Dec. 27, 2011).
75. Search of The Dru Sjodin National Sex Offender Public Website for Samuel L. Jackson, on December 1, 2011.
76. Answer at 8-9, Jackson v. InfoTrack, No. 11-cv-5801 (N.D. Ill. Sept. 16, 2011).
77. InfoTrack, Pre Employment Background Screening: Criminal Background Screening, **www.infotrackinc.com/screening-products.php** (last visited Oct. 6, 2011).
78. Notice of Acceptance of Offer of Judgment, Jackson v. InfoTrack, No. 11-cv-5801 (N.D. Ill. Nov. 29, 2011).
79. U.S. Census Bur., Population Division, *Genealogy*, **www.census.gov/genealogy/names/**.
80. Christensen v. Acxiom Info. Sec. Servs., Inc., 2009 WL 2424453 at *3 (W.D. Ark. 2009).
81. *Id* at *4.
82. *Id*.
83. *Id*.
84. *Id*.
85. *Id*.
86. Adam Liptak, *Expunged Criminal Records Live to Tell Tales*, N.Y. Times, October 17, 2006, *available at* **www.nytimes.com/2006/10/17/us/17expunge.html?pagewanted=all**.
87. *Id*.
88. SEARCH, National Task Force Report on Commercial Sale of Criminal Record Information, *supra* note 11 at 10-11.
89. Nate Carlisle, *Some Utahns find their expunged criminal past is still present*, Salt Lake City Trib., June 5, 2011, *available at* **www.sltrib.com/sltrib/news/51753949-78/expunged-criminal-expungement-utah.html.csp**.
90. *Id*.
91. The Associated Press, *AP IMPACT: When Your Criminal Past Isn't Yours*, N.Y. Times, Dec. 16, 2011, *available at* **www.nytimes.com/aponline/2011/12/16/technology/AP-US-TEC-Broken-Records.html?hp=&pagewanted=all**.
92. Complaint at 2-3, VanStephens v. ChoicePoint Work Place Solutions, Inc., No. 08 CV 952 (N.D. Ill. Feb. 14, 2008).
93. *Id*.; Answer at 3, VanStephens v. ChoicePoint Work Place Solutions, Inc., No. 08 CV 952 (N.D. Ill. Mar. 31, 2008).
94. Complaint at 3, VanStephens v. ChoicePoint Work Place Solutions, Inc., No. 08 CV 952 (N.D. Ill. Feb. 14, 2008).
95. Complaint, Ex. A (Cook County Contract with ChoicePoint), VanStephens v. ChoicePoint Work Place Solutions, Inc., No. 08 CV 952 (N.D. Ill. Feb. 14, 2008); Cook Co. Gen. Admin. Order No. 2002-03 Subject: Bulk Electronic Data Dissemination Policy, *available at* **www.cookcountycourt.org/rules/admin_orders/admin_orders_2002.html#02-3**
96. Deposition of Preg, *supra* note 66 at 116:9.
97. Complaint, Ex. C: USIS Background Check, Garcia v. USIS Commercial Services, Inc., No. 08-cv-01710 (N.D. Ill. May 8, 2008).
98. Complaint, Ex. B Rap Sheet, Garcia v. USIS Commercial Services, Inc., No. 08-cv-01710 (N.D. Ill. May 8, 2008).
99. Deposition of Ken Mittendorff, assistant director of the Dep't of Info. Sys., at the Supreme Ct. of Virginia, Office of Exec. Sec'y at p 69:22-70:5, Soutter v. Equifax Info Serv., 2011 WL 1226025 (E.D. Va. Mar. 30, 2011).
100. Soutter, 2011 WL 1226025 at *2.

101. *Id*. at *3.
102. Kim Zetter, *ChoicePoint's Checks Under Fire*, Wired Mag. (March 23, 2005), *available at* **www.wired.com/politics/security/news/2005/03/66983?currentPage=3**.
103. Carlisle, *supra* note 87.
104. *See, e.g.*, Comm'n on Public Access to Court Records, Report to the Chief Judge of the State of New York (Feb. 2004), *available at* **www.nycourts.gov/ip/publicaccess/Report_PublicAccess_CourtRecords.pdf**; North Dakota Supreme Court Comm., Court Tech. Comm., Requests for Bulk Data From District Court Case Information Systems (Mar. 12, 2003), *available at* **www.ndcourts.gov/court/committees/ct_tech/bulk.htm**; Texas Judicial Counsel, *supra* note 33.
105. Idaho Ct. R. 32(g)(27); Kan. Ct. R. 196(e); Neb Ct. R. § 1-801; S.D. Codified Laws §15-15A-11 (2005); Wash. Gen. R. 31(g)(3).
106. Ark. Sup. Ct. Admin. Order 19 § 6(B)(1)(b) (2010).
107. Ark. Sup. Ct. Admin. Order 19 § 6(B)(1)(a) (2010).
108. Ariz. Admin. Code §§ 1-605(D)(2), (D)(3) (2011).
109. 109 *Id*.
110. The Associated Press, *supra* note 91.
111. *Id*.
112. *See, e.g.*, New York Human Rights Law, N.Y. Exec. Law § 296 *et seq*. (McKinney 2010).
113. Federal Trade Commission, *supra* note 54 at 81, *citing* Allan, FTC Informal Staff Opinion Letter, May 5, 1999.
114. Criminal Justice Information Systems Regulations, 28 C.F.R. Part 20.
115. Paul L. Woodard and Eric C. Johnson, U.S. Dep't of Justice, Bur. of Justice Statistics, Compendium of State Privacy and Security Legislation: 2002 Overview, NJC 200030 (Nov. 2003)
116. U.S. Dep't of Justice, The Attorney General's Report on Criminal History Background Checks (June 2006).
117. Bur. of Justice Statistics, Survey of State Criminal History Systems, 2008, *supra* note 61 at 3.
118. *Id*. at 7.
119. SEARCH, National Task Force Report on Commercial Sale of Criminal Record Information, *supra* note 11 at 40.
120. *Id*. at 45.
121. *Id*. at 22-23.
122. Amended Complaint at 3-4, Doe v. ADP Screening and Selection Servs., Inc., No. 10-cv-06485 (W.D.N.Y. June 13, 2011).
123. *Id*.
124. Amended Complaint, Ex. A, Doe v. ADP Screening and Selection Servs., Inc., No. 10-cv-06485.
125. Amended Answer at 5, Doe v. ADP Screening and Selection Servs., Inc., No. 10-cv-06485 (W.D.N.Y. July 5, 2011).
126. Defendant ABSO's Motion for Summary Judgment, Affidavit of Denise Best, Stewart v. ABSO, Inc., 2010 WL 3853114 (W.D. Ky. 2010)
127. Stewart, at *10.
128. *Id*.
129. Community Legal Servs., Inc., Stories of Persons Hurt by Background Reports Produced by Commercial Vendors (Nov. 17, 2009) at Ex. B.
130. *Id*.
131. Complaint at 4-6, Smith v. HireRight Solutions, Inc., 2010 WL 2270541 (E.D. Pa. 2010).
132. Complaint, Ex. C: USIS Background Check, Garcia v. USIS Commercial Services, Inc., No. 08-cv-01710 (N.D. Ill. May 8, 2008).

133. Complaint at 3, Serrano v. Sterling Testing Sys., Inc., 557 F. Supp. 2d 688 (E.D. Pa. 2010).
134. Defendant's Memorandum of Law Motion To Dismiss, Serrano, 557 F. Supp. 2d 688.
135. Serrano, 557 F. Supp. 2d at 692.
136. NCLC Survey, *supra* note 27.
137. Phenix Group, Inc. (report on file with author).
138. Telephone Interview with Patricia Worth, Co-Director of Justice Strategies, Center for Community Alternatives (Oct. 17, 2011).
139. Deposition of Keith Alan Clifton at 44, Taylor v. Tenant Tracker Inc., 2010 WL 5174583 (E.D. Ark. Dec. 15, 2010).
140. Deposition of Stringfellow, *supra* note 63 at 87.
141. *Id*.
142. Deposition of Preg, *supra* note 66 at 64.
143. InfoTrack, Nationwide Criminal Database Search/Nationwide Sex Offender Registry Database Search, **www.infotrackinc.com/screening-products.php#nc** (last visited Dec. 15, 2011).
144. Wilson v. Rental Research Servs., Inc., No. 3-96-820, at 11 (D. Minn. Nov. 10, 1997*). See also* Taylor v. Tenant Tracker Inc., 2010 WL 5174583, (E.D. Ark. Dec. 15, 2010); Fiscella v. Intelius, Inc. 2010 WL 2405650 (E.D. Va. 2010).
145. Wilson, No. 3-96-820, at 11 (D. Minn. Nov. 10, 1997).
146. *Id*.
147. NAPSB, Background Screening Agency Accreditation Program Policies and Procedures (Oct. 2009) *available at* **www.napbs.com/files/public/Consumer_Education/Accreditation/BSAAP_PP122109.pdf**.
148. Pub. L. No. 111-203 (July 21, 2010).
149. Pub. L. No. 111-203 § 1088 (July 21, 2010); 75 Fed. Reg. 57252 (Sept. 20, 2010).
150. Pub. L. No. 111-203, § 1088(a)(1)(E), 124 Stat 1376 (July 21, 2010).

*Boston Headquarters:*
7 Winthrop Square
Boston, MA 02110-1245
Phone: 617/542-8010
Fax: 617/542-8028
www.nclc.org

NCLC®

NATIONAL CONSUMER LAW CENTER®

Advancing Fairness in the Marketplace for All

*Washington Office:*
1001 Connecticut Ave, NW
Suite 510
Washington, DC, 20036
Phone: 202/452-6252
Fax: 202/463-9462