CONSUMER DATA INDUSTRY ASSOCIATION
Empowering Economic Opportunity
Writer's Direct Dial: 202-408-7407
Writer's Email: eellman@cdiaonline.org

January 3, 2017

Centers for Medicare & Medicaid Services
Department of Health and Human Services
Attention: CMS–2404–NC
P.O. Box 8013,
Baltimore, MD 21244–8013

Re: Medicaid Program; Request for Information (RFI): Federal Government Interventions to Ensure the Provision of Timely and Quality Home and Community Based Service; CMS–2404–NC; RIN 0938–ZB33

Filed electronically at www.regulations.gov

To Whom It May Concern:

I write on behalf of the Consumer Data Industry Association ("CDIA") to offer comments on the above captioned matter ("RFI"), specifically as it relates to the question of criminal background checks. We have two points to offer CMS. First, name-based background checks by the private sector, as opposed to only a fingerprint check through the FBI, have been proven time and again to be the most comprehensive, current, and reliable way to check the background of a job applicant. Second, in addition to being more comprehensive, name-based background checks conducted by the private sector are governed by federal and state law and guidance and these laws offer greater protections to job applicants than the limited (if any) protections provided through a fingerprint check.

CDIA is well-placed to offer this comment. Founded in 1906, CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment screening, tenant screening and collection services. Our members include some of the largest

background check companies in the United States providing employers and landlords nationwide with background check reports containing, among other information, criminal history.

The RFI notes that the Centers for Medicare & Medicaid Services ("CMS") wants "to help improve the quality of care of home and community-based services (HCBS) provided to Medicaid beneficiaries." The RFI adds that "[p]ersonal care services ('PCS'), are a critical component of HCBS, and there is evidence of program integrity vulnerabilities in their provision."

In the RFI, the CMS asks "[w]hat issues should be considered in requiring criminal background checks? In the states that are utilizing fingerprinting and background checks already, what lessons can be learned from implementation and experience with these approaches?" CDIA can help answer the first part of the question and offer evidence to the superiority of name-based checks over fingerprint checks.

CMS is right to be concerned about crimes against those being served by PCS providers or attendants in home and community-based environments and to consider requiring criminal background checks for these workers.[1] As CMS knows all too well, for example,"[o]lder adults are particularly attractive targets for financial exploitation by unscrupulous individuals."[2] The U.S. Department of Justice noted that "[e]lder abuse and neglect is an understudied problem in the United States[,]" but, according to the Government Accountability Office ("GAO"), the "number of elder abuse reports and investigations in their states have been increasing steadily over the past few years."[3] The same concerns also apply to any home-based caregivers to the disabled.[4]

---

[1] HHS has seen evidence of criminal activity in other environments. *See*, Centers for Medicare & Medicaid Services, National Background Check Program, Long Term Care Criminal Convictions Work Group, Report, available at http://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-13-24-Attachment-.pdf ("*Work Group Report*"). The *Work Group Report* is an outgrowth of a March 2011 Office of Inspector General Report citing the prevalence of former convicts in the nation's nursing facilities. *Nursing Facilities Employment of Individuals with Criminal Convictions*, OEI-07-09-00110, March 2011 ("*OIG Report*").

[2] Government Accountability Office, *Elder Justice: National Strategy Needed to Effectively Combat Elder Financial Exploitation*, *GAO-13-110* (Nov. 2012).

[3] Government Accountability Office, *Elder Justice: Stronger Federal Leadership Could Enhance National Response to Elder Abuse,* GAO 11-208 (March 2011).

[4] *Home Health Care Agencies Conducted Background Checks of Varying Types,* Dep't. of Health & Human Services, Office of the Inspector General, OEI-07-14-00130 (May 2015), https://oig.hhs.gov/oei/reports/oei-07-14-00130.pdf.

1. **Name-based criminal background checks conducted by the private sector will offer more comprehensive protections to Medicare beneficiaries**

Since recipients of PCS are often in vulnerable positions CMS should exercise extreme caution in allowing those with criminal histories to provide care for those in need. It is for this reason that CDIA encourages CMS to recommend that providers of PCS undergo a name-based criminal background check conducted by the private sector.

The attached white paper gives CMS a sense of the value and comprehensive nature of name-based, private sector, criminal background checks. CMS should thoroughly review this paper to better appreciate how to best protect Medicaid beneficiaries. As we note in the paper, fingerprint checks are incomplete. For example, the FBI wrote that

> [a] search of commercially available databases may reveal charges and dispositions not reported to the state or national repositories [and] records relating to some offenses are not reported to the FBI…[5]

2. **Name-based criminal background checks conducted by the private sector will offer more comprehensive protections to PCS providers and attendants**

CMS should require that the criminal background check be conducted by a private company to ensure that the process offers the most comprehensive consumer protections available to the PCS providers and attendants. When a criminal background check is done by a private company, that search is regulated by the federal Fair Credit Reporting Act ("FCRA") and state FCRA laws.[6] Since 1971, the FCRA has served employers and applicants alike by, among other things, acknowledging vibrant and lawful use of criminal history information, requiring reasonable procedures to ensure maximum possible accuracy of reported information. The FCRA also provides job applicants and employees with certain disclosures related to background investigations. The law is also clear that applicants have the ability to access and correct any inaccurate or incomplete information in that background check reports.

The FCRA is "an intricate statute that strikes a fine-tuned balance between privacy and the use of consumer information."[7] When a criminal background check is done by the government or by the patient or family, consumers get no such protections

---

[5] The Attorney General's Report on Criminal History Background Checks, U.S. Dep't. of Justice, Office of the Att'y. Gen. (June 2006), 54, http://www.bjs.gov/content/pub/pdf/ag_bgchecks_report.pdf.

[6] 15 U.S.C. § 1681 *et seq*.

[7] Remarks of FTC Chairman Tim Muris, October 4, 2001 before the Privacy 2001 conference in Cleveland, Ohio. When a check is done by the FBI, no FCRA protections exist for consumers.

and employers have no assurances of the accuracy of reported information. There are no comprehensive, national accuracy, notice, or correction rights for consumers when a background check is done directly by the government, the patient or the family. This lack of protection leaves job applicants wondering how, when, and if they can see the result of the background check, and how, when and if they can get any errors corrected.

As an example of consumer protections, the FCRA provides that:

- Whenever a consumer reporting agency prepares a consumer report it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.[8]
- Whenever a consumer reporting agency reports public record information to an employer, such as criminal history, and that information will likely have an adverse effect on the individual's ability to obtain employment, the agency must either provide notice to the individual about such or follow strict procedures to insure the information is complete and up to date.[9]
- Consumers have a right to dispute information on their consumer reports with consumer reporting agencies and the law requires dispute resolution within 30 days (45 days in certain circumstances). If a dispute cannot be verified, the information subject to the dispute must be removed.[10]
- A consumer reporting agency that violates federal law is subject to private rights of action, enforcement by the Federal Trade Commission ("FTC") and Consumer Financial Protection Bureau ("CFPB"), and state attorneys general.[11]

In addition to the general protections above, there are protections specific to the use of consumer reports for employment purposes. The FCRA allows employers to request the criminal histories of prospective and existing employees for employment purposes.[12] However, this legal privilege comes with certain obligations. In short, under § 1681b(b) of the FCRA:

- An employer must certify to the consumer reporting agency that the employer has and will comply with the disclosure and authorization requirement as well as follow required steps in the event information in a consumer report may be used adversely against an applicant or employee. In addition, an employer must certify that the information from the consumer report will not be used in

[8] 15 U.S.C. § 1681k(e)(b).
[9] *Id.*, § 1681k.
[10] *Id.*, § 1681i(a)(1), (5).
[11] *Id.*, § 1681n, 1681o, 1681s.
[12] *Id.*, § 1681b(a)(3)(B).

violation of any applicable federal or state equal employment opportunity law or regulation.

- Employers must also provide an additional disclosure if a decision to not hire is made based on information in the consumer report so as to advise a job applicant or employee of their right to challenge the accuracy or completeness of the report.[13]

3. Conclusion

Name-based background checks by the private sector, as opposed to only a fingerprint check through the FBI, have been proven time and again to be the most comprehensive, current and reliable way to check the background of a job applicant. The attached white paper offers substantial information to help CMS reach that conclusion. CMS should also conclude that when background checks for PCS attendants are conducted, the checks should afford the maximum consumer protection to the subjects of the background checks. The only way to provide this consumer protection is when the background check is done by a private company and not by the government or the patient.

We hope that this information has been helpful to you. Please let me know if we can provide additional information or answer any questions.

Sincerely,

Eric J. Ellman
Interim President and Chief Executive Officer
Senior Vice President, Public Policy and Legal Affairs

[13] *Id.*, § 1681m(a).

Attachment

CDIA
CONSUMER DATA INDUSTRY ASSOCIATION
Empowering Economic Opportunity

Points in Support of
Name-Based and Private Sector Criminal Background Checks

Summary

This paper, supported by third-party research, studies, reports, and media stories, examines how and why criminal background checks performed by the private sector are more comprehensive and better at protecting the public than fingerprint checks from either the FBI or a state fingerprint database. The paper can be broken down in to several key parts: (1) The FBI database is incomplete; (2) While there are plenty of federal and state consumer protections for background checks conducted by commercial searches, there are no similar accuracy requirements placed on the government; (3) Fingerprint only searches of state government databases often suffer the same failings as the FBI database.

1. The FBI database is insufficient for a complete criminal check

A. Fingerprints searches are incomplete

While many people think the FBI and state law enforcement criminal history databases are the touchstones for all criminal history information, it is not. "The fingerprint identification process has what UCLA Law Professor Jennifer Mnookin describes as 'enormous cultural power,' exerting seemingly incontrovertible influence over juries, judges, and even innocent defendants"[1] as well as fans of television shows like CSI. While

> [f]ingerprint identification, long regarded as 'the gold standard for identifying criminals,' might be better analogized as an 'emperor with no clothes.' The reliability of fingerprint identification has never been comprehensively tested…Nor has the fingerprint-identification process's error rate been established or even estimated. Yet for the better part of a century, fingerprint identification has been accepted and admitted in court, remarkably without

[1] Note: *Fingerprint Identification: How "The Gold Standard of Evidence" Could Be Worth Its Weight*, 32 Am. J. Crim. L. 265, 266 (citing Jennifer Mnookin, *A Blow to the Credibility of Fingerprint Evidence,* Boston Globe, Feb. 2, 2004, at A14).

question.[2]

Checking the FBI database alone offers an incomplete picture into someone's criminal history. While the FBI database can be a source for criminal history information it should not be the only source. According to a U.S. Attorney General's report on background screening,

> The fact is that there is no single source of complete information about criminal history records. A check of both public and commercial databases and of primary sources of criminal history information such as county courthouses would, perhaps, provide the most complete and up-to-date information.[3]

The FBI database is not a case management system and frequently has only limited information; its best use is as a pointer for *possible* criminal records. The intent of the FBI database was to provide investigative leads based on fingerprint evidence, and not to produce employment screening reports.

The access to FBI records is through state agencies or via FBI approved entities, called "channelers". While these channelers can provide access to FBI data to entities that have statutory authorization to view that data, channelers themselves are not able to view FBI data. Employers are also not able to access FBI fingerprint systems.

The FBI keeps identifying information <u>voluntarily</u> submitted by many state and local criminal justice agencies in a database known as the Interstate Identification Index ("III" or "Triple I"). According to a report from the U.S. Attorney General,

> Contrary to common perception, the FBI's [III, or Triple I] system is not a complete national database of all criminal history records in the United States. Many state records, whether from law enforcement agencies or courts, are not included or have not been updated. For example, not all the state criminal history records…meet the standards for inclusion in the III. Because of inconsistent state reporting requirements, some criminal history records involve offenses that are not submitted to the FBI. Other records that were submitted to the FBI do not have fingerprints of sufficient quality to be entered into the system. Moreover, many criminal history records may contain information regarding an arrest, but are missing the disposition of that arrest. Currently, only 50 percent of III arrest records have final dispositions.[4]

---

[2] *Id*.

[3] The Attorney General's Report on Criminal History Background Checks, U.S. Dep't. of Justice, Office of the Att'y. Gen. (June 2006), 54, http://www.bjs.gov/content/pub/pdf/ag_bgchecks_report.pdf.

[4] *Id*., 16-17; See also 3.

The report added that

> [c]ommercial databases…offer other information that may not be available through state and FBI repository checks. A search of commercially available databases may reveal charges and dispositions not reported to the state or national repositories [and] records relating to some offenses are not reported to the FBI…Even state repositories may not have records on less serious offenses that have not been forwarded by local law enforcement agencies. Some of this information may be available through certain commercial databases.[5]

Name-based searches are critical to a criminal background checks and are superior to a finger-print only search. Commercial vendors rarely have access to fingerprint searches. Name-based searches can help identify attempted fraud or misrepresentation where an applicant attempts to circumvent their criminal history via the submission of false or incomplete information. In fact, in 2014, 43 states performed over 19.4 million name-based criminal background checks for non-criminal justice purposes.[6]

In 2008, Congress found that "[n]early 21 [million] criminal records are not accessible by NICS [the National Instant Criminal Background Check System] and millions of criminal records are missing critical data, such as arrest dispositions, due to data backlogs…The primary cause of delay in NICS background checks is the lack of…updates and available State criminal disposition records…and automated access to information concerning [misdemeanor convictions]."[7]

At a Congressional hearing in 2007, Assistant Attorney General for Legal Policy, Rachel L. Brand testified that the FBI's Triple I System has just 75% of all crimes committed in the U.S. and a mere 44% of that 75% have a final disposition.[8] That means that of all crimes in the U.S. only 33% of final dispositions are available from the FBI Triple I System.

---

[5] *Id*., 54.

[6] *Survey of State Criminal History Information Systems, 2014*, U.S. Dep't. of Justice, Office of Justice Programs, Bureau of Justice Statistics, Criminal Justice Information Policy, 10, https://www.ncjrs.gov/pdffiles1/bjs/grants/249799.pdf ("DOJ Survey, 2014").

[7] Pub. L. 110-180, § 2 (Jan. 8, 2008). NICS "is a computerized system that queries several national databases simultaneously in order to process a name-based background check. The databases checked include…the Interstate Identification Index (III or 'Triple I'), a database of criminal history records [and] the National Crime Information Center (NCIC). *Lethal Loopholes; Deficiencies in State and Federal Gun Purchase Laws: Hearing Before the Comm. on Oversight and Gov't. Reform,* 110th Cong. 1 (May 10, 2007), Serial No. 110-9 (Statement of Assist. Att'y. Gen. for Legal Policy, Rachel L. Brand) ("Lethal Loopholes"), 125.

[8] *Lethal Loopholes*, 146.

Attempts to fix the FBI's background check system are not working. Even though Congress passed the NICS Improvement Amendments Act of 2007, the proposed improvements "has never come close to the amounts called for by the [members of Congress]" and an unnamed source in the Justice Department said that the NICS record improvement had "gone to seed."[9]

Public policy tends to over-emphasize the value of FBI data at the expense of multi-jurisdictional searches performed by private background checks. The benefits of multi-state, multi-access points was shown in a 2011 GAO report. When the GAO looked at transportation security in 2011 at our nation's sea and airports, it found that "[s]tate repositories are considered more comprehensive sources of state criminal history than that maintained by FBI databases."[10]

The GAO also found that the Transportation Security Administration's

> visibility to applicant criminal history records [from the FBI] is often incomplete because the provided information excludes details regarding dispositions, sentencing, release dates, and probation or parole violations, among others. TSA reported that this lack of visibility to additional criminal history record information via the FBI's Interstate Identification Index system hinders its ability to fulfill its homeland security mission and conduct Security Threat Assessments with more detailed and complete information for its credentialing programs.[11]

In connection with its national transportation security review, the TSA told the GAO that it, the TSA, "conducted over 3 million Security Threat Assessments requiring a criminal history record check" and just north of 40 percent of the cases "included associated criminal records identified during automated FBI database".[12] This is a very low hit rate for a criminal database.

---

[9] Alex Yablon, *What Happened to the $1.3 Billion Congress Approved to Improve Federal Gun Background Checks?* The NICS Improvement Amendment Act of 2008 was intended to improve lapses in state record keeping that have allowed dangerous people like Dylann Roof to get a gun. Here's why almost 90 percent of that money has never been spent, The Trace, July 27, 2015, http://www.thetrace.org/2015/07/nics-background-check-congress-spending/.

[10] General Accountability Office, *Transportation Security: Actions Needed to Address Limitations in TSA's Transportation Worker Security Threat Assessments and Growing Workload*, GAO-12-60 (Dec. 8, 2011), 22, http://www.gao.gov/assets/590/586757.pdf ("GAO-12-60").

[11] *Id*., 30-31.

[12] *Id*., n. 54.

The GAO's concerns from 2011 did not go away when the GAO testified before Congress three years later. In congressional testimony in 2015, the GAO noted looked back at its 2011 report on transportation security and said that

> In December 2011, we found that, according to TSA, limitations in its criminal history checks increased the risk that the agency was not detecting potentially disqualifying criminal offenses as part of its Aviation Workers security threat assessments for airport workers. Specifically, we reported that TSA's level of access to criminal history record information in the FBI's Interstate Identification Index excluded access to many state records such as information regarding sentencing, release dates, and probation or parole violations, among others. [13]

The GAO added in that testimony that

> TSA and FBI officials, concluded that the risk of incomplete information did exist and could be mitigated through expanded access to state-supplied records. TSA officials reported that the FBI has since taken steps to expand the criminal history record information available to TSA when conducting its security threat assessments for airport workers and others.[14]

Not enough steps have been taken apparently. In 2014, the U.S. Department of Justice's Bureau of Justice Statistics ("BJS") found that:

- Twenty-nine states representing 59% of U.S. offenders reported that they are missing 40% of dispositions for arrests made in the preceding five years.
- For arrests older than five years, 31 states, representing 65% of all offenders in the nation's criminal history records, report that they are missing dispositions for over 40% of the arrests in their systems.[15]

Reporting dispositions is not improving. This BJS report from 2014 noted a 12% decrease in dispositions reported since the last report was issued in 2012.[16]

---

[13] *Hearing on Transportation Security: Are Our Airports Safe?: Before the House Committee on Oversight and Government Reform, House of Representatives*, May 13, 2015 (114th Cong.) (statement of Jennifer Grover, Director, Homeland Security and Justice, Gov't. Accountability Office) (citing GAO-12-60), https://oversight.house.gov/wp-content/uploads/2015/05/Ms.-Jennifer-Grover-Testimony-Bio1.pdf.

[14] *Id*.

[15] DOJ Survey, 2014, 2-3.

[16] *Id*., 6.

This report also looked at state participation in the FBI's National Fingerprint File (NFF). Here, 14 states that are NFF participants have elected not to forward to the FBI disposition information on second and subsequent offenses.[17]

In those cases where dispositions are reported to a central repository, the 2014 BJS found that 20 states have backlogs in entering court disposition data into their criminal history databases and at the time of the report, there were over 3 million unprocessed or partially processed court disposition forms from 19 states.[18]

The more one looks, the more one finds flaws in the FBI fingerprint database enhancing the need for name-based checks from the private sector. A 2012 congressional investigation revealed that "statewide databases that [the Office of Personnel Management] has approved [for national security clearance background checks] provide only cursory information, including the date of offense, charge, and disposition. These databases do not include information about the underlying facts that lead to an arrest."[19]

B. FBI Flaws Laid Bare: The Case of Dylann Roof

FBI database searches are not conducted in real time. Arrest information can take as much as 24 days to appear in the FBI system and court disposition information can take over a month, if it shows up at all. The private sector can generally respond to criminal background check requests much more quickly than the government can. This combination of speed and reliability places the right people in the right jobs in the right time.

The failures of the FBI database can have tragic consequences. CNN reported in June 2015 that

> Dylann Roof, the man who allegedly killed nine people in a Charleston church last month, should not have been able to buy a gun, the FBI has now determined, contradicting earlier assertions that the background check was done properly, a law enforcement official tells CNN and FBI's director told reporters in Washington.

---

[17] *Id*., 6.

[18] *Id*., 9.

[19] *Slipping Through the Cracks: How the D.C. Navy Yard Shooting Exposes Flaws in the Federal Security Clearance Process*, Staff Report, U.S. House Comm. on Oversight and Government Reform, Feb, 11, 2014 (citing, Transcribed Interview of Merton Miller, Associate Director, Federal Investigative Services (Jan. 8, 2014) at 201, https://oversight.house.gov/wp-content/uploads/2014/02/Aaron-Alexis-Report-FINAL.pdf.

. . .

> Due to a prior arrest when Roof admitted to possessing drugs, he should not have been permitted to buy the gun he used in the massacre. However, the NICS agent who was performing the background check on Roof was unable to determine which county the arrest had been made in and whether Roof had been convicted of the crime.

The CNN report also noted that the FBI check "took longer than three days to complete".[20]

2. Consumers are unprotected by FBI searches.

When a criminal background check is done by a private company, that search is protected by the federal Fair Credit Reporting Act (FCRA) and state FCRA laws. Since 1971, the FCRA has served employers and applicants alike by acknowledging vibrant and lawful use of criminal history information, requiring reasonable procedures to ensure maximum possible accuracy, and requiring substantial systems to correct any inaccuracies that occur. The FCRA is "an intricate statute that strikes a fine-tuned balance between privacy and the use of consumer information."[21] When a criminal background check is done by the government, consumers get no such protections. There are no comprehensive, national accuracy, notice, or correction rights for consumers when a background check is done by the government. This lack of protection leaves consumers wondering how, when, and if they can see the result of the background check, and how, when and if they can get any errors corrected.

3. Commercial searches are superior to state government-only fingerprint searches

Similar to the discussion above regarding FBI fingerprint searches there are problems with state-only searches, as well. The Florida Department of Law Enforcement conducted a head-to-head comparison of fingerprints and name-based searches. The Department found that

> The accuracy of the name hits is surprisingly high. This is particularly true because of the limitation that FDLE did not conduct name and demographic searches of alias names listed on the fingerprint card. . .The data shows that the

---

[20] Pamela Brown, Evan Perez, and Don Lemon, *FBI says Dylann Roof should not have been cleared to purchase a weapon*, CNN, July 10, 2015, http://www.cnn.com/2015/07/10/politics/dylann-roof-fbi-gun-south-carolina/.

[21] Remarks of FTC Chairman Tim Muris, October 4, 2001 before the Privacy 2001 conference in Cleveland, Ohio. When a check is done by the FBI, no FCRA protections exist for consumers.

> extremely high accuracy rate of the name searches makes these searches sufficient. . .When the IAFIS [Integrated Automated Fingerprint Identification System] or other automated fingerprint systems allow for very quick responses and low costs, fingerprint comparison will be the best option. Until then, name searches are the only practical option for determining criminal past.[22]

The value of information from the commercial sector is proven in many quarters beyond the U.S. Department of Justice. While not related specifically to criminal background checks the Texas Attorney General's office states, "[w]e need the private sector to help protect consumers and help combat identity fraud. Moreover, we also need the private sector to assist law enforcement."[23]

In March 2015, the GAO issued a report following over a year's worth of study on criminal background checks. According to the GAO, "[t]he use of private companies to conduct criminal history record checks appears to be increasing because [these checks] can provide benefits, such as faster response times."[24]

Then-FBI Director Louis Freeh testified before Congress in 1999 and noted that in 1998, his agency made more than 53,000 inquiries to commercial on-line databases "to obtain public source information regarding individuals, businesses, and organizations that are subjects of investigations." This information, according to Director Freeh, "assisted in the arrests of 393 fugitives, the identification of more than $37 million in

---

[22] Martha Wright, Chief of the User Services Bureau, Criminal Justice Information Services, Florida Department of Law Enforcement, *The Efficacy of Name-Based Searches For Other than Criminal Justice Purposes*, Florida Department of Law Enforcement, https://www.fdle.state.fl.us/Content/getdoc/e78560cd-8d70-4ac6-b24a-63a98d21d8ce/Wright.aspx, 10 ("FDLE Report"). In the study, the FDLE established

> [a] pilot program to test the efficacy of name-based searches. [In this pilot,] name-based searches and fingerprint searches were run on the same persons. There were 62,545 out of 62,545 cases (99.8%) where the resulting identification of a record was exactly the same regardless of which method of search and identification was used. When the Integrated Automated Fingerprint Identification System or other automated fingerprint systems allow for very quick responses and low costs, fingerprint comparison will be the best option. Until then, name searches are the only practical option for determining criminal past for persons who will have access to potential victims.

Id., 6.

[23] *Amicus Argument of James Ho for State of Texas*, *Taylor v. Acxiom Corp.*, U.S. Court of Appeals (5th Cir.) Case Nos. 08-41083, 41180, 41232, (Nov. 4, 2009).

[24] *Criminal History Records: Additional Actions Could Enhance the Completeness of Records Used for Employment-Related Background Checks*, GAO 15-162, i, http://www.gao.gov/assets/670/668505.pdf.

seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning."[25]

As stated by the Department of Homeland Security: "[W]e often get more accurate data from the commercial sector. In addition, the processes by which government agencies manage data often makes it difficult to acquire and needs [a] great deal of labor intensity into making it usable and accessible to other entities."[26]

4. Fingerprints are not foolproof

A. Fingerprints are vulnerable to hacking and spoofing

When the infamous bank robber, Willie Sutton, was asked why he robbed banks, he replied simply, "because that's where the money is."[27] If fingerprints are Coronado's illusive "gold standard"[28] than Fort Knox was robbed in 2015. The Washington Post reported that "[o]ne of the scariest parts of the massive cybersecurity breaches at the Office of Personnel Management just got worse: The agency now says 5.6 million people's fingerprints were stolen as part of the hacks."[29]

---

[25] *Hearing before the Senate Comm. on Appropriations Subcomm. for the Departments of Commerce, Justice, and State, and the Judiciary and Related Agencies, March 24, 1999 (Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation).*

[26] *The Privacy Office, Department of Homeland Security, Privacy and Technology Workshop, Official Transcript* at 6 (Sept. 8-9, 2005) (comments of Grace Mastalli Principal Deputy Director for the Information Sharing and Collaboration Program at DHS), available at http://www.au.af.mil/au/awc/awcgate/dhs/privacy_wkshop_panel1_sep05.pdf.

[27] See, https://www.fbi.gov/about-us/history/famous-cases/willie-sutton.

[28] See, Jonathan Saltzman, *Lawyer Cites Trouble With Fingerprints As Evidence, Boston Globe*, Feb. 6, 2004, at B1. See also Howard Manly, Prints Snafu in Cowans Case Almost Criminal, Boston Herald, Jan. 25, 2004, at 8 (describing how fingerprints "all but guaranteed the conviction of a suspect if his prints were near a victim or crime scene").

[29] Andrea Peterson, *OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought*, Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/. In 2015, the General Accountability Office wrote that

> Federal agencies' information and systems remain at a high risk of unauthorized access, use, disclosure, modification, and disruption. These risks are illustrated by the wide array of cyber threats, an increasing number of cyber incidents, and breaches of PII occurring at federal agencies. Agencies also continue to experience weaknesses with effectively implementing security controls, such as those for access, configuration management, and segregation of duties. OMB and federal agencies have initiated actions intended to enhance information security at federal agencies. Nevertheless, persistent weaknesses at agencies and breaches of PII demonstrate the need for improved security. Until agencies correct longstanding control deficiencies and address the hundreds of recommendations that we and agency inspectors general have made, federal systems will remain at increased and unnecessary risk of attack or compromise.

OPM is not the only fingerprint database subject to hacking. A recent major security flaw was exposed in Android phones allowing hackers access to fingerprint information on these devices.[30] In 2013, "[t]he biometrics hacking team of the Chaos Computer Club (CCC) has successfully bypassed the biometric security of Apple's TouchID using easy everyday means."[31] In 2002, [a] Japanese cryptographer has demonstrated how fingerprint recognition devices can be fooled using a combination of low cunning, cheap kitchen supplies and a digital camera."[32]

B. Fingerprints are not as one-size-fits-one as people think

Dave Aitel, a former computer scientist for the National Security Agency who specializes in offensive security for Wall Street financial firms, Fortune 500s and manufacturers, wrote in USA Today that "biometrics are often seen as a military-grade security technology. But in high security environments, biometrics are only a small part of the security puzzle. . . [F]ingerprint identification technology is not perfect - on a large enough database you will inevitably get collisions." Aitel added that "concerns about the statistical probability of false matches have been expressed by the National Academies of Science, National Institute of Standards and Technology, US Department of Justice, International Association for Identification, and more." [33]

New research is showing the weaknesses of fingerprint matching. "The language of certainty that examiners are forced to use hides a great deal of uncertainty," said the U.K.'s Lord Justice Leveson put it when addressing the Forensic Science Society. The scientific uncertainty of fingerprint matching is highlighted in a Pacific

---

General Accountability Office, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO-15-714 (Sept. 2015), 54.

[30] Thomas Fox-Brewster, *Samsung Galaxy S5 Flaw Allows Hackers To Clone Fingerprints, Claim Researchers*, Forbes, April 21, 2015, http://www.forbes.com/sites/thomasbrewster/2015/04/21/samsung-galaxy-s5-fingerprint-attacks/.

[31] Chaos Computer Club, Chaos Computer Club breaks Apple TouchID, *http://ccc.de/en/updates/2013/ccc-breaks-apple-touchid*, Sept. 21, 2013.

[32] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002, http://spie.org/Publications/Proceedings/Paper/10.1117/12.462719. . See, also, a 2003 presentation by T. Matsumoto at the Massachusetts Institute of Technology, http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf.

[33] Dave Aitel, Special for CyberTruth, *Why fingerprints, other biometrics don't work*, USA Today, Sept. 12, 2013, http://www.usatoday.com/story/cybertruth/2013/09/12/why-biometrics-dont-work/2802095/

Standard article backed up with research from the U.C.LA. Law Review, university professors, and report by the National Academy of Sciences.[34]

5. Limits of state law enforcement searches

Private-sector background screening ensures that the search is conducted across state lines and jurisdictions. This comprehensive searching is essential to ensuring that, for example, a violent crime in one state is not ignored when the same individual applies for a job in another state. One state agency search of crimes committed in that one state is of limited value in a country where people move across states with ease and frequency. A resident of one state may have been convicted of an offense in a second state and is now applying for a job with a company in a third state. A criminal background check conducted by a state government limited by the borders of its own state may, depending on the employer and the position, be considered to be inadequate and unsafe. For example,

> Florida conducts over 600,000 name-based record checks per year, but FDLE is authorized to access Florida information only. With the great mobility of our population today, a criminal history check of one state is very limiting. Name-based record checks should be examined to determine if the uses should be expanded to include nationwide information.[35]

In **Ohio**, law enforcement is stymied when clerks don't report convictions. In that state "thousands of convictions, which police officers and public and private employers hope to detect during background checks, are missing from the state database." A number of counties in the state "have not turned in the most-serious offenses — felony convictions — for three months and perhaps much longer, according to the May 1 audit." In was discovered during an "an investigation by WBNS-TV (Channel 10) and The Columbus Dispatch discovered major flaws in a criminal background-check system that periodically reports that felons have clean records."[36]

Ohio is not the only state law enforcement agency with issues. A 2011 audit of the **Texas** Department of Public Safety (DPS) showed that

---

[34] Sue Russell, Why Fingerprints Aren't the Proof We Thought They Were, Pacific Standard, Sept. 20, 2012, http://www.psmag.com/politics-and-law/why-fingerprints-arent-proof-47079.

[35] FDLE Report, 9.

[36] Randy Ludlow, *Law enforcement is stymied when clerks don't report convictions*, Columbus Dispatch, May 10, 2015, http://www.dispatch.com/content/stories/local/2015/05/10/law-enforcement-stymied-when-clerks-dont-report-convictions.html.

> the 73.68 percent submission rate indicates that data in DPS's Computerized Criminal History System is not complete, and users may not receive a reliable result from criminal history background checks that are conducted based on the data in that system. DPS also should improve the timeliness and accuracy of the data in its Computerized Criminal History System.
> . . .
>
> A significant number of prosecutor and court records are not reported to DPS, which impairs the quality of information that DPS uses to conduct criminal history background checks. For example, 1,634 (7.65 percent) of 21,351 offenders whom TDCJ admitted to jail, prison, or probation in November 2010 did not have corresponding prosecutor and court records in DPS's Computerized Criminal History System. In addition, information that DPS provides as part of its criminal history background checks does not include probation records.[37]

"**Washington's** criminal history records database is incomplete" so says a June 2015 audit by the Washington State Auditor's Office.[38]

The Washington State Auditor's Office audit showed that "[one-]third of the dispositions for charges reported in the Judicial Information System (JIS) in 2012 were missing from [the Washington State Identification System] WASIS." The audit also found that "more than half of the individuals with missing dispositions had at least one missing disposition for an offense on the state's Department of Social and Health Services' list of disqualifying offenses. These offenses include such crimes as harassment, child molestation and domestic violence."[39] More than one-in-ten of the missing dispositions were for felonies and 89% were gross misdemeanors, which also include offenses like stalking, shoplifting, animal cruelty.

The number one reason cited by the audit as to why "criminal history records are incomplete" is because "fingerprints are not taken".[40] The audit said that

> One reason fingerprints are not taken is a state law that does not require law enforcement entities to fingerprint individuals arrested for gross misdemeanors if they are not taken into custody. We also found that even when fingerprints are

---

[37] *An Audit Report on The Criminal Justice Information System at the Department of Public Safety and the Texas Department of Criminal Justice,* State Auditor's Office, SAO Report No. 12-002, Sept. 2011, available at http://www.sao.state.tx.us/reports/main/12-002.pdf.

[38] Performance Audit: *Improving the Completeness of Washington's, Criminal History Records Database*, Wash. State Auditor's Office, 11, June 15, 2015, http://www.sao.wa.gov/state/Documents/PA_Criminal_History_Records_ar1013675.pdf.

[39] *Id*., 3-4.

[40] *Id*., 4.

> taken, dispositions may not make it to WASIS because JIS allows dispositions to be entered without the [Process Control Number] PCN.[41]

There are other reasons why criminal history records are incomplete. The "[State] Patrol relies on hundreds of independent, local law enforcement agencies, courts and county clerks to provide the information needed to keep the state's criminal history records database…complete."[42] Yet, this diffusion of responsibility leads to incomplete records.

The incompleteness of these state records affects people. The audit points to an April 2015 incident where a bus driver, "carrying senior citizens on a day trip", "was arrested for [DUI]. He turned out to have a prior arrest for the same offense, which would have disqualified him from driving the bus. He did not mention the earlier arrest on his application and it did not appear on his background check because the offense was not in WASIS. This happened because he was cited and released for the prior offense; he was not booked into jail and fingerprints were not taken, resulting in the arrest not being entered into WASIS."[43]

"It turns out the State Patrol wasn't required to report the 2014 incident because the charge is a gross misdemeanor – and Maier wasn't taken to jail."[44]

According to an account of an investigation in 2014 in **Florida**,

> The Florida Department of Law Enforcement's troubled five-year-old automatic fingerprint identification system (AFIS) has cost far more to maintain than it did to design and build because of technical problems. It is now so unstable that it is causing delays during investigations and arrests across the state.
>
> . . .
>
> The most critical problems the internal reports document were related to the system's accuracy rates and response time. . . That meant the system

---

[41] *Id*., 4.

[42] *Id*., 6.

[43] *Id*., 15.

[44] Steve Kiggins, *How did a volunteer shuttle bus driver with DUI charge pass background check?*, KCPQ-TV, April 9, 2015, http://q13fox.com/2015/04/09/how-did-a-volunteer-shuttle-bus-driver-with-a-dui-charge-pass-a-state-background-check/.

> was missing as many as 13 prints in a batch of 1,300, which could add up to hundreds of prints in a day.[45]

Like Washington State, "the completeness of arrest and subsequent case disposition data in the ACCH [Arizona Computerized Criminal History] continues to be a concern among criminal justice stakeholders in **Arizona**." A 2013 report by the Arizona Criminal Justice Commission looked at

> the latest [Arizona Computerized Criminal History system] ACCH extract received…from [the state Department of Public Safety], 65.7 percent of arrest counts resulting from arrests made in calendar year 2009 had associated case disposition data attached to the record by the end of calendar year 2010 [and the] percentage of 2003 arrest counts…with associated case disposition information in the ACCH by the end of 2004 was 59.4 percent. Despite an increase over the seven-year period, there is still a large percentage of arrest counts entered each year that have not completed the case disposition process within the 180-day timeframe as outlined by the Arizona Supreme Court.[46]

The Arizona report noted the same challenge in inputting data for "cite and release" arrests as Washington State. The Arizona report noted that

> [m]any Arizona law enforcement agencies are faced with the task of patrolling a vast rural landscape within each of Arizona's 15 counties. As a result, many agencies are citing and releasing the arrestee in lieu of transporting the arrestee to a booking location. When a law enforcement officer issues an arrest citation and releases the arrestee, the arrestee is not fingerprinted, and the creation of a record of the arrest in the ACCH is delayed.[47]

A report issued in 2014 exposed a serious threat to public safety in Nevada. According to a study, "more than 800,000 criminal cases, some going back 20 years…were not forwarded by **Nevada** law enforcement agencies and the courts for entry into the state criminal information repository."[48]

---

[45] Tristram Korten, *State Fingerprint System Flawed, More Expensive To Maintain Than To Build*, blog, Florida Center for Investigative Reporting, March 9, 2014, http://fcir.org/2014/03/09/state-fingerprint-system-flawed-more-expensive-to-maintain-than-to-build-bondi-moye-barati-fdle-lave/.

[46] Arizona Criminal Justice Commission, *Identity Theft Arrest and Case Processing Data: An Analysis of the Information in Arizona's Computerized Criminal History Record System*, March 2013, 4, http://www.jrsa.org/webinars/presentations/az_id_theft.pdf (internal citations omitted).

[47] *Id*.

[48] Las Vegas Review-Journal, Report: Nevada repository missing thousands of criminal records, June 14, 2014, http://www.reviewjournal.com/news/nevada/report-nevada-repository-missing-thousands-criminal-records.

About the Consumer Data Industry Association (CDIA)

www.cdiaonline.org

CDIA is an international trade association, founded in 1906, of more than 130 corporate members. Its mission is to enable consumers, media, legislators and regulators to understand the benefits of the responsible use of consumer data which creates opportunities for consumers and the economy. CDIA members provide businesses with the data and analytical tools necessary to manage risk. They help ensure fair and safe transactions for consumers, facilitate competition and expand consumers' access to a market which is innovative and focused on their needs. CDIA member products are used in more than nine billion transactions each year.

December 2016