Compliance & Ethics PROFESSIONAL

Vol. 6 / No. 5
10 / 2009

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

TOP STORIES INSIDE

4 Incentivizing good compliance
By Lori A. Richards

18 Background checks: The essentials of personal due diligence

26 Reporting anticipated violations: SOX may not protect you

36 New Chinese anti-trust investigative rules set out "dawn raid" procedures

54 How much guidance does your organization provide its compliance and ethics investigators? A benchmarking survey

Meet Tony Boswell

Executive Director, Office of Compliance
City of Chicago

E-Verify bait & switch: Data mining isn't what employers signed up for

By Kevin Lashus and Robert Loughran

In a speech in Arlington, Virginia on June 16, 2009, Assistant Secretary of Homeland Security John Morton—the top Immigration and Customs Enforcement (ICE) Special Agent in the country—offered that he, "want[ed] employers to view ICE as a true partner to find ways to stay within the law." In light of the recent proposed rulemaking by the Department of Homeland Security (DHS), amending the Privacy Act, Freedom of Information regulations, and Notice of Privacy Act system of records, employers best view ICE as a partner who may be too close for comfort.[1]

Without notice, at the end of May 2009, DHS announced to the business community that it was establishing a system of records, a "Compliance and Tracing and Monitoring System (CTMS)" in order to data mine the required information provided by employers enrolled in E-Verify. The Verification Division of DHS created the Monitoring and Compliance (M&C) branch, which is responsible for both monitoring and referring faulty or failed compliance practices to ICE for administrative and criminal investigation. Once monitoring analysts identify perceived "non-compliant behaviors," a notification will be forwarded from CTMS to ICE Special Agents to conduct a follow-up investigation. Through a concurrently issued DHS regulation, "DHS proposes to exempt portions of the CTMS from one or more of the provisions of the Privacy Act because of criminal, civil and administrative enforcement requirements." The basis for the exemption is detailed in the regulation: the data in E-Verify will be used for law enforcement activities.

Although the Department of Homeland Security provided the public 30 days to comment, the effective date of the regulations coincided with the submission date for comments—June 22, 2009. DHS did not wait to consider the business community's concern about the regulations prior to implementation.

In this article, we will discuss the background of E-Verify, the consequences of the data mining, and consideration which should be made prior, during, and after an employer agrees to enroll in the E-Verify system.

E-Verify: A primer

In 1996, the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRAIRA) created E-Verify (originally designated in the statute as the "basic pilot program").[2] Recently, E-Verify was extended and its statutory authority is currently designated to terminate on September 30, 2009.[3]

The following entities are currently required to participate in E-Verify:

- All employers doing business in Arizona, Mississippi, and South Carolina;
- State employers and state contractors in Colorado, Idaho, Georgia, Minnesota, Missouri, Nebraska, Rhode Island, and Utah; and,
- State employers in North Carolina.

By Executive Order, all federal contractors and their sub-contractors (with exceptions) will need to use E-Verify to confirm that all of their new hires and their current employees who work in furtherance of the federal contracts are authorized to legally work in the United States.

The current E-Verify program arose from the same legislative intent of the Immigration in the National Interest Act of 1995 (INIA). The Report of the Judiciary Committee correctly identified that, "[w]hile most employers try to comply with the law, it is impossible for honest employers to distinguish genuine documents from high-quality (but inexpensive) counterfeit ones."[4] It was the purpose of the INIA to assist employers to root out document fraud, and nothing more. The bill explicitly prohibits the system from requiring a "national I.D. card" and from any use other than to verify eligibility to work or to receive certain government benefits, or to enforce criminal statutes related to document fraud.

The government announcement of data mining is a unilateral contractual modification of the Memorandum of Understanding that 120,000 employers have already signed with the federal government. This radical shift exposes E-Verify participants to criminal employer sanctions charges, as a result of a program being used in a manner that is opposite of its original intent. To suggest that employers may be a little unprepared for the modification is a bit of an understatement. To understand the impact of the modification, we must first identify the data mining efforts and then determine whether pro-active remediation is required.

History of E-Verify compliance and monitoring efforts

In 2002 in its INS Basic Pilot Evaluation, Summary Report,[5] Westat informed the government that employers did not always follow the correct procedures and that some engaged in practices such as:

- pre-employment screening,
- acting adversely against employees who did not immediate clear the system,
- missing deadlines,
- failing to inform employees of their rights, and
- failing to terminate employees who did not clear the system.[6]

Similar information was again reported by Westat in its September 2007 report, entitled "Findings of the Web Basic Pilot Evaluation." In response to these continuing problems, Westat reported that the US Citizenship and Immigration Services (USCIS) had established monitoring and compliance units in 2007.[7]

The US Government Accountability Office (GAO) reported, as of April 2008, the USCIS Monitoring and Compliance branch had 21 investigative staff and planned to hire 32 additional staff in fiscal years 2008 and 2009.[8] The GAO stated that by January 2009, USCIS had plans to establish a regional verification office with 135 staff members to conduct status verification and monitoring and compliance activities. The USCIS, Monitoring and Compliance branch's stated mission was to: (1) prevent fraud, discrimination, or illegal use of E-Verify; (2) educate employers and provide assistance with compliance procedures; (3) follow up with employers on misuse of the system; and (4) monitor E-Verify system usage and refer identified instances of fraud, discrimination, or illegal use of the system to enforcement authorities such as ICE or the Department of Justice's Office of Special Counsel.[9]

GAO noted that the Monitoring and Compliance branch could help ICE better target its worksite enforcement efforts. ICE officials noted that they had requested and received E-Verify data from USCIS on specific employers who participate in the program and are under ICE investigation. USCIS also reported that by monitoring the use of the E-Verify program prior to June 2008, USCIS staff was able to identify instances of fraudulent use of Social Security numbers and referred such examples of fraud to ICE.[10]

In June 2008, GAO also reported that USCIS and ICE were negotiating a Memorandum of Agreement (MOA). This agreement was finalized in December 2008.[11] Pursuant to this agreement, the USCIS Verification Division is charged with the following duties:

- Identification and pursuit of suspected employer and employee misuse, abuse, and fraudulent use of E-Verify, and the tracking and management of all such cases.
- Referral of suspected employer and employee misuse, abuse, and fraudulent use of E-Verify to ICE for investigative consideration, in particular cases of a specific incident or pattern or practice of:
  - Misuse, abuse, and/or fraudulent use of E-Verify occurring at critical infrastructure sites;
  - Violations regarding employment of unauthorized aliens;
  - Criminal activity (harboring offenses);
  - Failure to use E-Verify for all employees; or
  - Retaining employees after an E-Verify Final Nonconfirmation.

According to the MOA, both USCIS and ICE may conduct concurrent compliance activities, but ICE retains the right to suspend USCIS activities.

In May 2009, in the proposed regulation, the USCIS Verification Division announced creation of the Monitoring & Compliance (M&C) Branch.[12] The Branch has two core functions, monitoring and compliance, each with its own set of examples of "investigatative" leads.

CONTINUED ON PAGE 44

 CONTINUED FROM PAGE 43

Monitoring & Compliance

M&C personnel will utilize electronic "data mining" tools to research records created by E-Verify users in order to document suspected instances of the following for further investigation:

- **Fraudulent use of Alien-numbers and Social Security numbers,** by identifying multiple uses of the same data.
- **Termination of an individual's employment** based on an initial, "tentative non-confirmation" result, as indicated by a large number of uncontested tentative non-confirmations.
- **Failure to notify the government when an employee is retained** after receipt of a Final Nonconfirmation, based upon unclosed cases or delayed closures of cases with a Final Nonconfirmation result.
- **Use of E-Verify on existing employees**, based upon verification and hire dates, multiple verifications of an employee, or a high number of verifications resulting in blank or invalid closure codes. (Most employers could trip this particular investigative flag when attempting to data enter existing employee's data from what are often incomplete historical records.)
- **Pre-screening of applicants**, based on a higher than expected number of queries.
- **Selective use of E-Verify**, based upon either too few verifications or a high number of foreign country codes in a user's E-Verify account.

Impact of new data mining procedures

During the verification process, compliance failures occur; sometimes, as a result of employer error, and sometimes as a result of a successful identity fraud by a newly hired employee. What makes the failures more dangerous in light of the data mining activity is the speed at which USCIS will be able to identify the failure and refer the case to ICE for investigation. Before an employer may be able to identify the failure during a routine review of its compliance policies, and remedy the failure internally, ICE may already be investigating the employer for significant worksite-related enforcement violations—essentially depriving an employer of its entitlement to a good-faith defense.[13]

A diligent employer, faced with the prospect of covert government monitoring that potentially results in a waiver of its Fourth Amendment protections, may instead focus its efforts on identifying prospective employees from a "safer" pool of job applicants. This precarious prospect was identified by the Court in *Collins Foods International, Inc. v. U.S. INS*:

> [The Immigration Reform and Control Act of 1986] is delicately balanced to serve the goal of preventing unauthorized alien employment while avoiding discrimination against citizens and authorized aliens. . . . [the] ultimate danger [is that many employers] faced with conflicting demands of the EEOC and the INS would simply avoid interviewing any applicant whose appearance suggests alienage.[14]

This conflict was also identified in the comments of a group of minority-led opponents to the IIRIRA E-Verify amendments urging the opposition to H.R. 2202:

> The 'verification system' is no answer to the problem of discrimination. In order to avoid the disruptions resulting from government errors and discrepancies, employers would most likely continue to avoid including individuals whose appearance, name, accent or family background make their profile appear 'foreign'.[15]

Obviously, discrimination during recruitment is not the answer. It is only a matter of time before most employers are compelled to E-Verify their workforces. Prudent employers will engage an audit of the employment verification documentation to identify compliance failure, and remedy the failure—before CIS refers the employer to ICE for investigation.

Recommendations for employers

For employers who are enrolled (or will be) in E-Verify, time is of the essence. The safest way for employers and senior management to protect their businesses and to help avoid personal liability for civil and criminal sanctions associated with employment eligibility verification compliance failures—which will be readily identified as a result of the government's data mining activity—is to retain

CONTINUED ON PAGE 46

 CONTINUED FROM PAGE 44

experienced immigration counsel to assist the employer in developing a consistent and meticulous Form I-9 verification and re-verification process. Experienced immigration attorneys should guide employers through an audit of existing I-9 Forms, ensuring that correctable errors are appropriately mitigated, and protecting the employer from additional liability with the shield of the attorney-client privilege.

Legal counsel should strongly advise clients to pursue attorney-supervised audits of I-9 Forms for all employees, company-wide. For an employer to reasonably calculate its active exposure throughout the process, it requires experienced counsel to determine the existence of technical and substantive errors under the applicable laws and to track the number of those errors remedied during the mitigation process.

During every phase of the employment eligibility verification process, counsel should be available to provide recommendations on all issues, from the collection of information on new employees to any other Form I-9–related inquiries that arise during initial Form I-9 completion or re-verification. Counsel should be prepared to provide customized legal advice in relation to adverse employment action, when required under federal law, and should prepare the company for the possible fluctuation in the labor pool that may result from the audit. Real-time exposure analysis and liability estimates should be determined under all legal regulations and should be carefully tracked during the audit process, so that the company may properly evaluate the exposure created in the past and the amount of liability that has been reduced by proper mitigation.

It is recommended that anyone involved in the process undergo a comprehensive I-9 training, conducted by competent counsel, so that each of these designated specialists may become experienced in the intricacies of employment eligibility verification. The verification process has become increasingly complex. Employers must recognize that even the most well-intentioned individuals may attract both civil and criminal liability, not only upon themselves, but also upon the company executives and to the company itself for failure to follow the verification process accurately and completely.

The primary purpose of an audit is to remedy compliance failures in an expeditious fashion to minimize exposure. Accordingly, the key is to commit to the audit in a manner that—as much as possible—best insulates the results from disclosure. Unless a full-scale audit is conducted as expeditiously as possible, an employer may be exposed to allegations of "knowing hire" or "reckless disregard" related to unauthorized employees.

In a matter involving employer sanctions, the lawyer must have all available information in order to devise strategies to best handle any compliance failures and to conduct an audit, so that the client is as compliant as possible, all the while trying to avoid consequences like mass disruptions in the labor supply. The privilege encourages full disclosure of this information by creating this trusting, confidential relationship.[16]

As it relates to an employer's audit of its I-9 Forms, in order for the exposure analysis identified by the audit to be protected from disclosure pursuant to the attorney-client privilege, the audit must have been conducted for the purposes of rendering legal advice or assistance.[17] The underlying purpose of the privilege is to allow clients to receive the most competent legal advice from fully informed counsel. This is particularly true when those implicated in the alleged wrongdoing maintain a good faith belief that their actions were appropriate and in the organizations best interest.[18] Generally speaking, a thorough Form I-9 audit involves continual legal analysis of detailed fact patterns which are not easily compartmentalized and require interactive legal evaluation and attorney-directed remediation. Merely having an attorney review an audit report may not protect it from disclosure.[19]

Additionally, audit results may be protected from disclosure by the work product doctrine, under which the audit results and any related materials are confidential and are not subject to disclosure if they reflect an attorney's legal strategy and thought processes. Investigations and audits may be protected from discovery if they are prepared "in anticipation of litigation," even if not directed by legal counsel and even if no lawsuit was filed at the time, as long as litigation is reasonably anticipated and not merely speculative.[20] Courts have consistently held that the "investigation by a federal agency (such as ICE—in light of its recent stepped-up enforcement activity) presents more than remote prospect of future litigation, and provides reasonable grounds

CONTINUED ON PAGE 48

 CONTINUED FROM PAGE 46

for anticipating litigation sufficient to trigger application of the work product doctrine."[21] Unlike the attorney-client privilege, the work product doctrine may extend to protect materials prepared "in anticipation of litigation" by non-lawyers who have assisted lawyers in the audit process.[22]

Although human resources managers or other employees may be helpful to the Form I-9 verification and audit processes, the work performed and knowledge gained by an attorney-led audit is protected by the attorney-client privilege. When experienced immigration attorneys lead an audit—unlike non-lawyer company owners, employees, or third-party non-lawyers—experienced counsel may make recommendations about hiring before the mitigation process of the audit commences, thus saving the employer from the potential of the resulting labor shortages attributable directly to the discovery of unauthorized workers on the payroll. The company may also able to limit the information discovered during the audit on a need-to-know basis as is determined by the employer's General Counsel. The determination of when sufficient information has been accumulated to take an employment action based on a determination which clears discriminatory hurdles and meets the reasonable employer standard should be carefully guarded by General Counsel.

This compartmentalization may also limit potential constructive knowledge charges on those who would be required to dismiss unauthorized workers immediately. In other words, for the audit to be successful, employees who may not be members of the control group for privilege purposes, may nevertheless come upon information—like an estimate of administrative or criminal exposure—that may be subject to disclosure. When the audit is conducted under the privilege provided by experienced counsel, such information, like the overall exposure, is still subject to the privilege, because it is not discoverable beyond the members of the control group.

Implementing a thorough Form I-9 policy and immigration attorney-led audit is the proactive step employers can take to ensure compliance with lawful hiring practices, especially considering the fundamental shortcomings of the electronic employment verification databases and the potential impact that could result from unscrupulous inspection. Assuming that some of the technical and substantive violations contained in the forms may be corrected uniformly under the proper supervision, the employer may reduce administrative exposure by hundreds of thousands of dollars by committing to a proper process of remediation. By involving an experienced immigration attorney in the Form I-9 auditing and mitigation process, companies can employ a best practices model that will be consistent company-wide and may also be protected by the additional benefits of the attorney-client privilege. ✦

Kevin Lashus is a Senior Attorney in the FosterQuan, LLP office in Austin, TX, and an Adjunct Professor at the University of Texas School of Law. He has also served as an Assistant District Counsel with the U.S. Department of Justice, Immigration and Naturalization Service, as well as an Assistant Chief Counsel with the U.S Department of Homeland Security, Immigration, and Customs Enforcement. Kevin may be contacted via e-mail at: klashus@fosterquan.com or by phone at 512-852-4130.

Robert Loughran is a Managing Shareholder and heads the Emigration and Employer Sanctions practice areas of FosterQuan, LLP from its Austin and Houston, TX offices. His practice is concentrated in the areas of corporate immigration, emigration abroad, and related international law. *Texas Monthly* has recognized Mr. Loughran as a Texas Super Lawyer. Robert may be contacted via e-mail at rloughran@fosterquan.com or by phone at 512-852-4142.

Notes

1 See DHS Docket No. DHS-2009-0015 and DHS Docket No. DHS-2009-0013, 74 Fed. Reg., No. 98, pages 23957-23958 and 24022-24027 (May 22, 2009).

2 Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA), Pub. L. 104-208, 110 Stat. 3009 (Sept. 30, 1996).

3 Pub. L. 111-8, Div. J, §101, Mar. 11, 2009.

4 Immigration in the National Interest Act of 1995, H.R. REP. 104-469(I), H.R. Rep. No. 469(I), 104TH Cong., 2ND Sess. 1996, 1996 WL 168955 (Report from Mr. Hyde, member of the Committee on the Judiciary).

5 Available at http://www.uscis.gov/files/nativedocuments/INSBASICpilot_summ_jan292002.pdf

6 Available at http://www.uscis.gov/files/nativedocuments/INSBASICpilot_summ_jan292002.pdf, pages v-vi.

7 Available at http://www.uscis.gov/files/article/WebBasicPilotRprtSept2007.pdf. See pages 157-159.

8 Statement for the Record of Richard M. Stana, Dir. Homeland Security and Justice Issues, To the Subcommittee on Immigration, Citizenship, Refugees, Border Security and International Law, Committee on the Judiciary, House of Representatives, Employment Verification, Challenges Exist in Implementing a Mandatory Electronic Employment Verification System. June 10, 2008 (GAO-08-895T). See page 18.

9 Id.

10 Id. at 19-20.

11 Available at http://www.uscis.gov/files/nativedocuments/USCIS-ICE-E-Verify%20MOA.pdf.

12 74 Fed. Reg., No. 98, pages 24022-24027, 24023 (May 22, 2009).

13 See IIRIRA (411); INA § 274A(b)(6); 8 U.S.C. § 1324a(b)(6), as amended.

14 948 F.2d 459 (9th Cir. 1991). Available at http://www.usdoj.gov/eoir/OcahoMain/publisheddecisions/Hardbound/Volume1/123.pdf

15 Additional Views Concerning Employment Verification System, 1996 In Crowd Comments to the Illegal Immigration Reform and Immigrant Responsibility Act, Pub. L. 104-208, 110 Stat. 3009 (Sept. 30, 1996).

16 Stephen Ellmann, Truth and Consequences, 69 FORDHAM L. REV. 895, 901 (2000).

17 See In re *Colton*, 201 F. Supp. 13, 15 (S.D.N.Y. 1961), aff'd, 306 F.2d 633 (2d Cir.1962), cert. denied, 371 U.S. 951 (1963); see also, VII J. Wigmore, Evidence, § 2292, at 558 (McNaughton Rev. 1940) ("are at [its] insistence permanently protected").

18 See N. Richard Janis: "Deputizing Company Counsel as Agents of the Federal Government." WASHINGTON LAWYER, Mar. 2005, at 32; Michael Farber: "Interviewing Company Employees in the Internal Investigation: Navigating the Minefield." 19 INSIGHTS 10 (2005); John Gibeaut: "Junior G-Men: Corporate Lawyers Worry that They're Doing the Government's Bidding While Doing Internal Investigations." 89 ABA J. 46, 51 (2005) ("[C]orporate lawyers are particularly worried that Justice is trying to drive a wedge between companies and employees."); Michael Burr, et al: "The CLT Top 20: The Events, People & Stories of 2005." 15 CORP. LEGAL TIMES 36, 42 (2005) (citing the August 2005 KPMG deferred prosecution agreement as the fifth most significant legal development in 2005 because it represents the larger problem of attacks on attorney-client privilege due to government demands for waiver of the privilege).

19 C.f. *Deel v. Bank of America*, 227 F.R.D. 456, 459-61 (W.D. Va. 2005) (where company conducted a self-audit of its payroll practices while FLSA litigation was pending, the attorney-client privilege protected documents sent to in-house or outside counsel for legal advice, including documents relating to the self-audit, a draft employee questionnaire, and drafts of the employee notices about the questionnaire. But, the completed questionnaires were not protected because the company "did not clarify to the employees completing the questionnaire that it needed the information to obtain legal advice.") with *Hardy v. New York News*, 114 F.R.D. 633 (S.D.N.Y. 1987) (where company's equal employment manager created documents about its minority employment goals and consulting firm, then analyzed the work done and created draft affirmative action plans. These documents were discoverable in subsequent litigation because an attorney did not direct their preparation or prepare the documents).

20 *Jeffers v. Russell County Board of Education*. Case No. 3:06 CV 685-CSC (M.D. Ala. Oct. 4, 2007)(protecting school board's investigation of sexual assault and harassment claims).

21 See, e.g., *Scurto v. Commonwealth Edison Co.*, 1999 WL 35311, at *2 (N.D. Ill. Jan. 11, 1999) (quoting Pacamor Bearings Inc. v. Mineba Co., Ltd., 918 F. Supp. 491, 513 (D.N.H. 1996)); see also In re Grand Jury Subpoena, 220 F.R.D. 130, at *147(D. Mass. 2004).

22 *United States v. Nobels*, 422 U.S. 225, 238-39 (1975).