LawLogix™

Top 5 Things You Need To Know About Identity Fraud and E-Verify

WHITE PAPER

Top 5 things you need to know about identity fraud and E-Verify

In November 2013 the United States Citizenship and Immigration Services (USCIS) announced an enhancement to the E-Verify system to help address the fraudulent use of Social Security numbers (SSNs) during the hiring process. While this change is undoubtedly good news to privacy advocates and individuals alike, employers must still be vigilant in protecting their employees' sensitive information especially in light of recent shifts in worksite enforcement.

LawLogix has assembled these 5 tips to help you prepare.

1 E-Verify has difficulties detecting identity theft

Although E-Verify is designed to confirm US employment eligibility, the system has long been criticized for its inability to detect (or prevent) cases of identity theft. This weakness stems from the fact that E-Verify does not actually authenticate the identity of the person presenting the documents, but instead simply compares it with information stored in various federal databases.

During the past few years, E-Verify has introduced various enhancements to combat this risk, including the photo matching tool, the E-Verify integration with certain state DMVs, and this latest enhancement relating to SSNs. While each one of these changes has improved E-Verify's accuracy, there is a still a possibility that an identity thief could "game the system" by creating phony documents which can be used to obtain "legitimate" IDs.

2 Employers participating in E-Verify have a contractual obligation to secure sensitive data

When employers enroll in the E-Verify system, they must sign a non-negotiable Memorandum of Understanding (MOU) which requires them to protect employee data that is transmitted to/from the E-Verify system. In particular, employers must closely restrict access to E-Verify data, ensure that it is not used for any other purpose, and generally protect its confidentiality on a need to know basis. It's also important to note that E-Verify data is governed by the Privacy Act and the Social Security Act; as such, any person who obtains this information under false pretenses or uses it for any purpose other than as provided for in the MOU may be subject to criminal penalties.

Guardian

LawLogix

3 E-Verify can refer cases of possible E-Verify fraud to various law enforcement agencies without notifying the employer

Under the E-Verify statute, the Department of Homeland Security is required to monitor E-Verify submissions in order to ensure the security and integrity of the E-Verify system. In order to satisfy this obligation, the DHS has established the "Monitoring and Compliance" branch which is responsible for monitoring and analyzing E-Verify transactional data to look for possible instances of abuse. In particular, the M&C Branch can refer instances of possible fraud, discrimination, and illegal or unauthorized activities to other federal agencies, such as Immigration and Customs Enforcement (ICE), the Department of Justice, and/or the Office of Special Counsel (OSC). As such, employers should take care in monitoring their own use of E-Verify in order to prevent any "surprise visits" by the government.

4 I-9 and E-Verify Audits often involve instances of identity theft

Since 2009, ICE agents have been increasingly using Form I-9 inspections for instances when they suspect the use of fraudulent documents but lack the means to obtain a criminal search warrant. By utilizing I-9 inspections, ICE may be able to uncover patterns of identity theft, fraudulent use of documents, or bad-acting human resource officials who facilitate or encourage such behavior.

5 A carefully crafted I-9 and E-Verify policy should address instances of identity theft

Immigration attorneys routinely recommend that employers create detailed I-9 and E-Verify "Standard Operating Procedures" that specify how an employer should deal with social security no-match letters, E-Verify TNCs, and suspected cases of identity theft (whether they arise through the E-Verify system or from external sources).

Attorneys also recommend that employers use smart electronic I-9 systems which include E-Verify alerts and reports which can help detect and prevent instances of possible abuse. In particular, a well-designed system should include automatic validation of Social Security numbers at the point of I-9 entry to ensure that the SSN is not already being used in the company, and to spot instances of SSNs which have never been issued.

Please visit our library of resources at *www.lawlogix.com/library* for everything I-9 and E-Verify related.

Click Here **to learn how Guardian By LawLogix can help your organization reduce errors and improve efficiency.**

Guardian™

LawLogix™