



New IRS and SSA Data-Sharing Efforts Raise Immigration Stakes for Employers: 5 Action Items to Address Risk

Insights

4.17.25

Federal authorities are ramping up their use of interagency data to pursue immigration enforcement, with major implications for employers. An April 7 agreement between the IRS and ICE enables immigration agents to access tax filings to support non-tax criminal investigations – particularly when it comes to worksite enforcement. The next day, the Social Security Administration announced it was repurposing its “death master file” – which is typically used to identify deceased individuals – to financially disable certain migrants whose legal status has been revoked. These developments reflect a coordinated strategy to drive self-deportation and intensify enforcement using data once considered off-limits, raising the stakes for employers across multiple industries. What are the five action items you should consider to address this new risk?

What’s New: IRS and SSA Agreements with Immigration Authorities

Two developments from last week will require you to reassess your immigration compliance efforts.

IRS–ICE Information-Sharing Agreement

On April 7, the IRS entered into a Memorandum of Understanding (MOU) with Immigration and Customs Enforcement (ICE), authorizing the disclosure of certain tax records for use in non-tax criminal investigations. The agreement provides ICE access to information such as Individual Taxpayer Identification Numbers (ITINs), wage filings, and employer-submitted forms – particularly W-2s and 1099s. While the data cannot be used for civil immigration enforcement or deportation proceedings, it is expected to support investigations into document fraud, identity theft, and unauthorized employment.

SSA “Ineligible Master File” Initiative

Separately, the Social Security Administration (SSA) has begun flagging certain noncitizens whose legal status was recently revoked, such as those formerly granted parole or temporary work authorization, as “ineligible” within systems traditionally used to identify deceased individuals. These individuals may have their Social Security numbers rendered invalid for financial and employment purposes. The policy, while reportedly focused on individuals with criminal records or security concerns, could expand in scope to include just about any worker.

Together, these efforts signal a broader federal strategy to combine siloed data sources – long shielded by privacy protections – to support aggressive enforcement initiatives.

Key Employer Exposure and Risk

Employers could face increased government scrutiny as agency coordination grows, ranging from administrative problems to higher-stakes enforcement activity:

- **Increased SSA “No-Match” Letters** – As SSA tightens data integrity efforts, employers may receive more letters flagging discrepancies between names and SSNs on wage reports. These notices do not imply wrongdoing but can create operational and legal complexity.
- **Greater Risk of Worksite Audits** – ICE and IRS may target employers whose filings suggest a pattern of undocumented labor, such as multiple ITIN-linked wage statements, repeated SSN mismatches, Affordable Care Act (ACA) reporting discrepancies with SSNs, or sudden spikes in contractor filings.
- **ICE Raids and Warrants** – Cross-referenced IRS and SSA data may be used to plan worksite raids or issue judicial warrants targeting high-risk locations. These actions may disrupt operations and draw media attention.
- **Potential Criminal Charges** – Employers found to have knowingly hired or facilitated unauthorized work may face prosecution under:
 - **8 U.S.C. § 1324a** (unlawful employment of unauthorized workers)
 - **8 U.S.C. § 1324** (harboring or transporting undocumented individuals)
 - **18 U.S.C. § 1001** (false statements on federal forms)
 - **26 U.S.C. § 7206** (filing false or fraudulent tax documents)

While criminal charges have historically been rare, this new IRS and SSA data-sharing initiative – along with the increased threat of prosecution under the new administration – adds pressure for employers to act cautiously and document compliance efforts.

5 Action Items for Employers

Employers should act now to minimize risk and prepare for potential inquiries by taking these five steps:

1. Conduct a Compliance Audit

Work with your FP counsel to review your I-9 documentation, ACA reports, payroll systems, and tax filings to ensure consistency. Confirm that all employment records are properly completed and stored.

2. Train HR and Managers

Equip frontline personnel with guidance on lawful document review and avoid practices that could result in document abuse or discrimination claims. They need to know how to complete I-9

forms, recognize document issues, and take appropriate action if they suspect an employee may lack proper work authorization.

3. **Prepare for Government Notices**

Develop internal protocols to respond to SSA no-match letters, IRS discrepancy letters, ICE audits, immigration enforcement subpoenas, and judicial warrants. Remember that inconsistencies between I-9s, ACA reporting, payroll records, and IRS submissions may inadvertently flag themselves for investigation, even when the cause is innocent. Responding improperly – or not at all – can create further liability.

4. **Review ITIN and 1099 Use**

If your business issues 1099s to individuals with ITINs, assess the nature of the relationship and whether the individual is properly classified. Consult your FP immigration counsel if gray areas arise.

5. **Develop a Response Plan**

Designate a team that is familiar with the mechanics of ICE audits and enforcement raids. [This resource is a good place to start](#). Your team should know how to contact legal counsel and prepare messaging for employees in the event of a raid, subpoena, or public inquiry. They should also know to contact Fisher Phillips' [Employers' Rapid Response Team](#) (877-483-7781 or DHSRaid@fisherphillips.com) at any time.

Looking Ahead: Policy May Shift, But Risk is Real

While litigation or legislative oversight may challenge aspects of these agreements, you cannot rely on political uncertainty to shield you. The trend toward data-driven enforcement is well underway – especially actions that leverage artificial intelligence (AI) technology and data analytics principles. Regardless of whether such information-sharing becomes a permanent part of our new reality, you need to take proactive steps to minimize your risk today.

Conclusion

If you have any questions about these developments or how they may affect your business, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our [Immigration Practice Group](#). Our [Employers' Rapid Response Team](#) (877-483-7781 or DHSRaid@fisherphillips.com) is on call to provide immediate legal counsel when a raid occurs, assist with documentation and compliance review, and provide post-raid support and strategy assistance.

Visit our [New Administration Resource Center for Employers](#) to review all our thought leadership and practical resources, and make sure you are subscribed to [Fisher Phillips' Insight System](#) to get the most up-to-date information.

Related People



Jocelyn Campanaro

Partner

303.218.3667

Email



David S. Jones

Regional Managing Partner

901.526.0431

Email





Shanon R. Stevenson

Partner

404.240.5842

Email

Service Focus

Immigration

Government Relations

Employers' Rapid Response Team for DHS Raids

Trending

New Administration Resource Center for Employers