

Immigration Update: The Future of Employment Verification

Lynden D. Melmed

With millions of Americans out of work, the immigration battleground this year will not be about legalization and how to address the millions of unlawful immigrants already in the United States. Instead, the immigration debate will center on whether the United States should mandate electronic worker verification to protect and free up jobs for Americans.

The new Republican majority in the House of Representatives wasted little time in establishing the new theme. Lamar Smith (R-Tex), the Chairman of the House Judiciary Committee which oversees immigration, responded to the President's State of the Union address by saying "it's hard for [the President] to talk about creating jobs and then endorse illegal workers keeping their jobs at the expense of American workers." The House Judiciary Committee's first two oversight hearings: worksite enforcement and the capabilities of the current, voluntary electronic verification system (E-Verify).

Representative Elton Gallegly (R-Calif.), the head of the House Judiciary Subcommittee on Immigration Policy and Enforcement, introduced two bills that would further expand the mandate that federal contractors use the current electronic verification system (E-Verify). And at the state level, Governor Rick Scott (R-FL) signed an executive order within an hour of becoming Florida's 45th governor that requires that certain employers and contractors in his state to use E-Verify.

Employment Verification Equals Job Creation

For decades, lawmakers have viewed employment verification as one pillar of comprehensive immigration reform, the most effective and humane way to control the flow of illegal migration. By removing the magnet of employment, unlawful immigrants will be less likely to make the journey to the United States.

But continued high unemployment is causing a shift in how some legislators talk about employment verification. Lawmakers at both the federal and state level are increasingly promoting employment verification not just as tool to reduce illegal immigration, but also as a means to create jobs for unemployed Americans. They argue that enforcing immigration laws and removing existing unlawful workers from the workforce will free up hundreds of thousands of jobs for legal workers. It is a powerful policy point: it makes no difference to someone looking for work if a job vacancy is created through economic growth or because the prior job-holder was fired because they were not authorized to work in the United States. Representative Smith made the point earlier this year, stating:

According to the national numbers, out of work Texans are most affected by illegal immigrants in the workforce. But millions of Americans across the nation are still struggling to find work. If the Obama administration would simply enforce the law, we could make millions of jobs available for out of work Americans

Deficiencies in Current Electronic Verification System

Since 1986, it has been illegal for employers to knowingly hire immigrants who are unauthorized, to work in the United States. The Immigration Reform and Control Act of 1986 (IRCA) established the Form I-9 process, which requires employers to verify documents presented by new employees to establish their identity and employment eligibility. An employer must accept a document if it reasonably appears to be genuine and to relate to the individual. With dozens of different acceptable documents, it has been, and continues to be, easy for unlawful immigrants to defeat the paper-based system and secure employment, even when the employer follows the law.

In 1996, Congress established a pilot electronic verification system. Originally called Basic Pilot and later renamed E-Verify, the largely voluntary system requires participating employers to complete the normal Form I-9 process and then manually enter certain data into the web-based E-Verify system. E-Verify then transmits the information to Social Security Administration (SSA) and Department of Homeland Security (DHS) databases to verify whether the individual is work authorized. Participation in E-Verify has grown rapidly over the past few years and the system continues to mature. From October 2009 through August 2010, E-Verify processed approximately 14.9 million queries from nearly 222,000 participating employers.

But E-Verify was never intended to address identity fraud, and its capabilities are limited when unauthorized workers present legitimate documentation of employment-authorized individuals. In those situations, neither the employer nor the databases are able to determine if employees are presenting genuine identity and employment eligibility documents that are borrowed or stolen. In one well-known immigration worksite raid, DHS identified over a thousand unauthorized workers in that workforce, even though the employer actively participated in the E-Verify system.

Identity Theft and Fraud: Different Strategies, No Consensus

Despite the decades-long recognition of the need for a mandatory employment verification system, and the renewed focus on expanding that system to free up jobs for U.S. workers, there is a surprising lack of consensus amongst legislators, business coalitions and advocacy groups as to what that that system should look like. The discord runs deeper than just when and how a mandatory verification system should be expanded. There is a fundamental disagreement about the structure of the system and,

more specifically, how the next generation of the electronic verification system will address identity theft and fraud.

One could attribute some of the discord to legislative strategy, as opponents of mandatory employment verification might advocate for alternative approaches to draw away support for proposals that are gaining momentum. But the merits of the competing proposals suggest that there is more than just legislative strategy at play, and that there are meritorious but fundamentally different concepts for how the next generation of employment verification should work. A successful system will need to prevent unauthorized workers from gaining access to the U.S. workforce, but it will also need to reduce identify theft and safeguard civil rights.

The following three proposals reflect the competing views and demonstrate how much work must be done by Congress before we will see a universal, mandatory verification system that addresses identity theft.

I. Expand and Improve E-Verify

Any debate about electronic verification understandably starts with E-Verify. Each year, there are proposals in Congress to expand E-Verify and make it mandatory for all employers. Numerous states have also imposed obligations on employers to utilize the current federal verification system, at times even imposing obligations that go further than the federal mandate. This legislative activity suggests that there is some political support for expanding and improving the current system.

But even proponents of E-Verify recognize that the system was never intended or designed to address identity theft. Because E-Verify is based on the paper I-9 process, it will confirm all employees as employment authorized as long as the information entered into E-Verify matches DHS and SSA records.

Nevertheless, DHS has been creative in trying to reduce the program's susceptibility to identity theft and fraud. One tool is photo matching, which relies upon photographic data already in the possession of the federal government. USCIS provides the photographic data to the employer so that the employer can determine whether the document presented by the new hire matches the document in the government system.

The photo tool has been around since 2007, and it places the burden on employers to determine whether the photograph on the employee's permanent resident card or employment authorization document matches the digitally stored photograph within DHS databases. If the employer determines that the photos do not match, E-Verify rules require that the employer indicate in the system that the photographs do not match, and the employee is to receive a tentative non-confirmation after which point the employee is to be provided with an opportunity to contest the determination. According to USCIS, from October 2009 to August 2010, there were 393,574 cases that initiated E-Verify's photo matching tool. Of these cases, employers indicated that 1,569 employees' photos did not match. *See GAO-11-146 (December 2010).*

In September 2010, USCIS added photographs of passport holders in State Department records to the E-Verify system. And for several years now, USCIS has been negotiating with states to gain access to driver's license data for E-Verify. USCIS will soon begin a pilot with the Motor Vehicle Association in one state that will allow an employer to verify a new employee's driver's license directly with the issuing agency. However, it appears that the pilot program will only share driver's license data and not the photographs. USCIS also intends to develop a program that would allow victims of identity theft to "lock" their Social Security numbers within E-Verify until they need them to obtain employment authorization. *See GAO-11-146 (December 2010).*

In strict terms, none of these tools utilize biometric authentication to validate the employee's identity. But in combination, they do reduce fraud and identity theft and make it increasingly difficult for unlawful immigrants to secure employment. And the anti-fraud initiatives build upon a system that has been around for 15 years and has been recognized for a high level of accuracy. USCIS data indicate that about 97.4 percent of almost 8.2 million newly hired employees were immediately confirmed as work authorized by E-Verify during fiscal year 2009, compared to 92 percent during June 2004 through March 2007. Though even a small error rate could result in problems for thousands of work-authorized Americans, no competing system offers a higher level of accuracy or reliability.

Some continue to call for the incorporation of biometric authentication into E-Verify. The 2009 Westat evaluation of E-Verify recommended "exploration of the use of biometrics to prevent identity fraud ... using fingerprints or other biometric checks." And James Ziglar, former USCIS Commissioner, told Congress in 2009 that "it would border on irresponsible not to seriously analyze the possibility of incorporating a biometric identification and verification module into the E-Verify system." But the most recent GAO report on E-Verify recognized the challenges that come with incorporating those tools, including the costs to design, develop, test and implement the system, as well as the costs to employers for purchasing and maintaining the hardware and software.

And even in its current form, E-Verify has its fair share of critics. The program is so controversial in Rhode Island that its incoming Governor, Lincoln Chafee, abolished it in January — just a day after Governor Scott ordered Florida to adopt it. Chafee said E-Verify, which had been in place for two years, had become a "divisive issue causing unnecessary fear and anxiety in our immigrant community."

II. New Employee Verification Act (NEVA)

The New Employee Verification Act (H.R. 5515) was introduced by Rep. Sam Johnson (R-TX) on February 28, 2008. NEVA aims to eliminate the voluntary E-Verify system of employment verification and replace it with a two-tiered system. The first tier contains no biometric element, but does direct the Social Security Administration to establish the Electronic Employment Verification System (EEVS), which would expand the National Database of New Hires (NDNH) to include workers' immigration status. Congress created NDNH in 1996 to help states track absentee parents and enforce outstanding

child support orders; 90 percent of US employers now submit data on new hires to the system. Information for recently hired employees would be checked against Social Security and Department of Homeland Security databases to determine work eligibility. The system would eliminate the I-9 immigration form.

Alternatively, employers could register for the Secure Electronic Employment Verification System (SEEVs), a network of government-certified private sector companies that would authenticate a workers' identity through a biometric identifier like a thumbprint. Employers that use SEEVs would be required to use government certified private sector entities called "enrollment providers" to provide identity authentication utilizing immigration and identifying information maintained by the SSA and DHS combined with background screening verification using publically available information. The law would mandate that biometric data maintained in SEEVs be encrypted and segregated from the identifying information and linked to the identifying information only by the consent of the new employee.

A key benefit of NEVA is that it would place the development of the biometric system in the hands of the private sector, which some believe is better situated to develop cost-efficient, technologically-advanced options. Additionally, many privacy advocates and libertarians are more comfortable with a biometric model if the information is not shared with or maintained by the federal government. The proposal also enjoys the support of several large business group coalitions.

The flexibility of private-sector development is also its legislative weakness, as the bill does not prescribe how the verification and biometric authentication process will operate. That uncertainty might be a sticking point for elected officials, who are already skeptical of the government's and the business community's commitment to a robust verification system.

III. BELIEVE System

In 2009, Senators Schumer and Graham (R-SC) joined forces to draft a comprehensive immigration reform bill. Though the political partnership ultimately faltered (but has since rekindled?), Senator Schumer has continued to promote his concept to develop a new tamper-proof ID card that *all* employees – U.S. citizens and foreign workers alike – would be required to obtain and present to employers to work in the U.S.

The Schumer model would replace E-Verify with a system called Biometric Enrollment, Locally-stored Information, and Electronic Verification of Employment ("BELIEVE"), which would be implemented within six years of enactment.

The concept was first unveiled in an op-ed in March 2010:

[The proposal] would require all U.S. citizens and legal immigrants who want jobs to obtain a high-tech, fraud-proof Social Security card. Each card's unique biometric identifier would be stored only on the card; no government database would house everyone's information. The cards

would not contain any private information, medical information or tracking devices. The card would be a high-tech version of the Social Security card that citizens already have.

Prospective employers would be responsible for swiping the cards through a machine to confirm a person's identity and immigration status. Employers who refused to swipe the card or who otherwise knowingly hired unauthorized workers would face stiff fines and, for repeat offenses, prison sentences.

Under the proposal, the Social Security Administration would begin issuing biometric social security cards within eighteen months of enactment. The cards would be fraud-resistant, tamper-resistant, wear resistant, and machine-readable social security cards containing a photograph and an electronically coded micro-processing chip which possesses a unique biometric identifier for the authorized card-bearer.

Employers hiring workers in the future would be required to use the newly created Biometric Enrollment, Locally-stored Information, and Electronic Verification of Employment (BELIEVE) System as a means of verification. Prospective employees would present the machine-readable, fraud proof, biometric Social Security card to their employers, who would swipe the cards through a card-reader to confirm the cardholder's identity and work authorization.

There are numerous benefits to this model. Employers would only accept one document (as opposed to 26 different documents they must accept today), and there would be an efficient system to swipe the new card and determine work status. By removing subjective determinations, employers would be less likely to intentionally or unintentionally discriminate during the hiring process.

Absent legislative text or other additional details, it is difficult to project the full cost of the proposal or fully understand how the process will operate. And until there is broad public debate, we won't know whether the desire to remove unlawful workers from the workforce has sufficient public support to justify requiring every U.S. citizen to submit their fingerprints to the federal government. Immigration is a passionate issue, but not necessarily for a majority of Americans. Will most Americans line up to provide fingerprints to the Department of Homeland Security?

On the other hand, new technology, such as iris scans, may make this option less invasive and more palatable, as fingerprints are often associated with criminal activity and background checks. And people are increasingly comfortable using biometrics in their daily life (e.g. fingerprint readers on personal laptops) and subjecting themselves to increased screening to secure employment (e.g. drug testing, credit and criminal background checks).

Conclusion

No one will benefit more than employers from an immigration overhaul that restores the rule of the law in the workplace and provides sufficient access to a legal workforce. The overwhelming majority of employers already invest substantial resources in their verification and compliance processes and they want to be on the right side of the law - it makes good business sense. In today's political and economic environment, those same employers don't want to hire – or even be perceived as hiring – unlawful workers. Employers need and want the federal government to provide them with the means to verify employees' identities and work authorization by comparing workers' identity documents with information in federal databases - either an improved E-Verify system or a similar program that achieves the same end.

One can easily imagine a scenario where Congress incorporates elements of all three proposals: (i) a measured expansion of E-Verify with improved anti-fraud tools capabilities in the near term, (ii) pilot programs to explore private sector or private-public options for biometric verification, and (iii) a long-term effort to incorporate biometrics into Social Security cards or other government-issued documents, which employers would then biometrically authenticate at time of hire.

If Congress is successful in designing and implementing an employment verification that is fast, accurate and addresses identity theft, it will be much easier to find common ground on how to phase-in such a system. Debating when and how to implement the next generation of an employment verification system, without first agreeing on what that model will look like, will likely continue the stalemate in Congress.

But employers will support the new system only if they have access to a legal workforce – an open question when the economy recovers and current immigration quotas limit the availability of legal workers. Congress should therefore carefully coordinate expansion of E-Verify, or any alternative system, with broader reforms that provides employers with a legal supply of workers they need to sustain and grow their businesses.

Summary:

Expand and Improve E-Verify:

- Integrates additional anti-fraud tools into the current, voluntary E-Verify system to reduce identity theft.
- Shares photographic data and driver's license data already in the possession of federal and state governments with the employer. With photo tool, employer then compares (i) the photographs on the document, (ii) the photograph in the data system, and (iii) the job hire. Enables the employer to better determine whether the document was issued to the person standing before them.
- USCIS is exploring other options to address identity theft, including tools that would lock certain social security numbers to prevent their unauthorized use.
- E-Verify continues to be controversial and opponents question the accuracy rate of the underlying data. Even with the anti-fraud initiatives, there is no “air tight” biometric system to eliminate identity theft.

NEVA:

- Eliminates E-Verify and moves verification process to the National Database of New Hires (NDNH).
- Creates a voluntary biometric program called Secure Electronic Employment Verification System (SEEVS), which would be run by a network of government-certified private sector companies that would authenticate a workers' identity through a biometric identifier like a thumbprint.
- Bill does not establish which biometric technology will be utilized, nor does it explain how the biometric system will operate.

BELIEVE:

- Eliminates E-Verify in favor of the Biometric Enrollment, Locally-stored Information, and Electronic Verification of Employment (BELIEVE) System.
- Social Security Administration would begin issuing new biometric social security cards to all workers (U.S. citizens and foreign workers alike) that contain a fingerprint images that are stored in the cards (not in a federal database)
- Employers would have scanners and would swipe the new biometric card at time of hire, which would validate both work authorization and identity.
- Proposal will have to overcome questions regarding cost, appetite for all Americans to provide biometrics to the government, and timeline for implementation.

Author Bio:

Lynden Melmed is a Partner in the Washington, D.C. office of Berry, Appleman & Leiden LLP (BAL). Prior to joining BAL, Mr. Melmed served as Chief Counsel of U.S. Citizenship and Immigration Services (USCIS), that agency's highest ranking legal position. He also served as Special Counsel to Senator John Cornyn (R-Texas), who at the time was Chairman of the Senate Subcommittee on Immigration, Border Security and Citizenship. He is a graduate of the University of Virginia (B.A., J.D.).