

Austin T. Fragomen, Jr.
Partner of the Firm

Direct: +1 212 891 7501
afragomen@fragomen.com

Fragomen, Del Rey, Bernsen & Loewy, LLP
7 Hanover Square
New York, NY 10004-2756
Main: +1 212 688 8555
Fax: +1 212 480 9930
www.fragomen.com

May 31, 2011

Via electronic mail
Steve.Degrow@mail.house.gov

Hon. Sam Johnson, Chairman
U.S. House of Representatives
Committee on Ways and Means
Subcommittee on Social Security
1102 Longworth House Office Building
Washington D.C. 20515

Re: Response to post hearing questions

Dear Chairman Johnson:

Thank you for the honor of testifying before the Subcommittee on April 14, 2011, and for this opportunity to answer follow-up questions in your May 17 letter. I respectfully submit the following response in the same order in which you posed the questions.

- 1. What is a solution for having a good employment verification system, one that does not put individual jobs in jeopardy due to its shortcomings, like failing to detect identity fraud and preventing an unscrupulous employer from lying to the system and certifying an unauthorized worker?*

Protecting American jobs and ensuring integrity of our immigration system can be achieved through a reliable verification system that prevents identity fraud. Indeed, a reliable electronic verification system is a cornerstone to preventing unauthorized employment in the United States. Furthermore, we need a system that minimizes burdens on honest employers so that resources can go to research, job creation, and not just compliance with paperwork requirements.

Employers need a verification system that tells them two things: 1) whether the person is who he or she says she is; and, 2) whether the person is authorized to work. U.S. workers need the government to help them quickly remedy any mistakes in the databases so they can get back to work. There also must be a true safe harbor for employers, not just from prosecution, but also

from the adverse consequences of unknowingly having unauthorized personnel. Instability in the workforce results in loss of productivity and revenue which ultimately hurts the American workers.

The time is ripe for the Department of Homeland Security (DHS) to pursue aggressively pilot programs to eliminate identity fraud and protect employers. Last Thursday, the U.S. Supreme Court ruled in Chamber of Commerce v. Whiting that Arizona's eligibility verification and E-Verify requirements were not preempted by federal law. This decision realistically will lead to one of two results – either Congress enacts stronger federal preemption language as part of E-Verify expansion legislation, or states will rely on the Supreme Court's holding to pass E-Verify and verification legislation even more aggressively than they do today. In either scenario, there will be greater E-Verify mandates, and DHS must address the identity fraud loophole in order for E-Verify to have any credibility among its participants. We believe the federal government, and not the states, is best positioned to test ideas and determine what is the most effective and efficient system to meet our national priorities on immigration.

We believe that the technology exists to greatly reduce the identity theft in the employment verification system. As explained in my testimony and as the chairman of this subcommittee envisioned in his New Employee Verification Act (NEVA), biometric technology is one good way to achieve this objective and is worth pursuing. Regardless of what technology DHS chooses, the bottom line is that the system and technology must prevent identity fraud and provide employers with certainty.

Finally, the Supreme Court's ruling last week underscores the need for the strongest possible federal preemption statute. Many job creators in the United States do business in several states. It can be very burdensome and confusing to them when states impose additional immigration compliance requirements, especially when these state laws are inconsistent with one-another and with federal law.

- 2. You pointed out that there are 60 million new hires annually, and that given job turnovers, most individuals would be verified within three to four years. What are the concerns employers have regarding E-Verifying their entire workforce?*

American employers understand they have an important role to play in securing our nation's borders and worksites. Yet, the government must acknowledge that there are substantial costs to employers when they assume this role. Businesses constantly have to balance the costs and benefits of undertaking any task. Reverification of the existing workforce is one area where the costs are likely to outweigh greatly the benefits, both to the nation and to most employers.

E-Verify as it exists currently can be an effective tool for matching a name with a Social Security number (SSN). It is not yet effective in uncovering identity fraud. Therefore, requiring employers to reverify their current employees through E-Verify would not guarantee the legality of the workforce. Also, as employers follow up on SSN no-match letters, a large number of currently unauthorized workers using false numbers will be discovered, and anyone who cannot

be detected through the SSN no-match letter process will not be detected through E-Verify anyway. Furthermore, there are many sectors that attract very few, if any, unauthorized workers so mandatory reverification yields no benefit to them at all. As many federal contractors have discovered in complying with the E-Verify amendments to the Federal Acquisition Regulation (FAR), the cost of using E-Verify on an existing workforce can be considerable, sometimes reaching into millions of dollars for the largest employers. Alternatively, if Congress does mandate reverification of the current workforce, the scope should be limited. At the very least, those hired prior to the enactment of the Immigration Reform and Control Act (IRCA) in November of 1986 should be exempt.

Moreover, as I testified on April 14, there is always a concern about “scalability,” meaning whether the system can accommodate a tremendous surge in usage. Currently, only about 3% of the U.S. employers are enrolled in E-Verify and, except for certain federal contractors, they may use it only for new hires. The surge in usage will be astronomical if all employers are required to use it for the entire workforce. DHS must not only assure the public that the system will be ready for the surge, but explain to Congress and the employer community exactly *how* it will accommodate the surge. Otherwise, the administrative cost associated with trying to deal with system errors and inefficiencies also will have an adverse effect on productivity and job creation.

In sum, while industries that frequently struggle with SSN mismatch issues among its workers may welcome the opportunity to use E-Verify on existing workers, many other sectors derive little or no benefit at all. It would not be good public policy to compel all employers to spend resources on reverification that otherwise can be used to grow their businesses and hire more workers. Reverifying the entire workforce, therefore, should be an option, but not a mandate, for employers.

3. The Department of Homeland Security (DHS) has just implemented a third party authentication system called Self Check. What is your assessment of the system?

Self Check is a great concept and was included in NEVA. It gives potential job seekers the opportunity to discover errors before they have to undergo E-Verify when reporting to a new job. This reduces or eliminates the burden on compliant employers and legal employees of having to resolve erroneous E-Verify non-confirmations. Of course, Self Check is only useful to compliant employers and legal workers. It is not intended as an enforcement tool against unscrupulous employers or unauthorized workers perpetrating identity fraud. Employers also are not permitted to require the use of Self Check.

Self Check is only available in Colorado, Idaho, Mississippi, Arizona, Virginia and the District of Columbia presently. Only employees logging on from an internet protocol (IP) address in one of these jurisdictions can use it. It is far too early to say whether the program will have significant impact on the overall verification process. More observation and analyses also are needed before assessing whether and how Self Check can be improved. DHS also should evaluate further the Self Check program and determine where it can be enhanced and developed

into a tool that is even more helpful to U.S. workers and employers, not just to residents of the above six jurisdictions.

4. *DHS has also just entered in a pilot program with the State of Mississippi where an employer could match an employee's driver's license photo against the state's database. As the driver's license is the one photo ID most people can present, does this idea hold any promise for better authentication? While the project has not yet begun, after a[n] acceptable time period for testing, how would you define a successful pilot?*

The photo screening tool should be among the pilots that DHS aggressively pursues. It is an important first step but is not enough. Until Mississippi's agreement to participate, photo screening tool's coverage had been limited to DHS-issued employment authorization documents (EAD), "green cards," and U.S. passports.

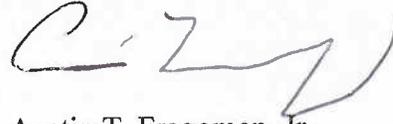
Undeniably, it makes perpetrating identity fraud more difficult. However, the photo screening tool currently has two major limitations. First, its scope is not wide enough. To avoid triggering the photo screening function on E-Verify, an unauthorized worker can present a fraudulently obtained document other than a passport, green card or EAD. If a fake driver's license is needed, the unauthorized worker would obtain one purporting to be from any jurisdiction other than Mississippi.

Second, the photo screening tool is only effective in detecting illegal photograph substitutions. The screening is limited to comparing the photograph on the computer screen with the photograph on the document presented. An unauthorized worker still may defraud a state to issue a document under a stolen identity and pass the photographic screening. Furthermore, employers still remain vulnerable as they have to exercise discretion and decide whether the images on the photographs match the persons physically before them.

This is not to say that the photo screening tool can never be effective. After the Chamber of Commerce v. Whiting decision, one would expect the states to become even more engaged in preventing identity fraud and ensuring data accuracy for verification purposes. Thus, whether E-Verify's photo screening tool can become a credible option will depend on DHS's ability to expand the program to all states and territories, and the state government's willingness to meet certain standards (e.g. Real ID compliance) to ensure the integrity of the documents they issue. In addition to just the photographs, E-Verify should authenticate driver's license numbers as well. Though this will not be as reliable as using biometric features, it is an idea worth pursuing if we lack the political will to explore a biometric pilot. The program also must extend to all identity documents acceptable for I-9 purposes so one cannot circumvent the screening. In addition, its function cannot stop at merely matching two photographs, but must ascertain whether the photograph is in fact the likeness of the person being verified. To serve the ultimate purpose of ensuring integrity at the worksite and protecting American jobs, the photo screening tool (or any other DHS pilot) must provide employers a safe harbor from government penalties and adverse economic consequences.

Once again, I thank you and your subcommittee staff for your kind invitation and for all your diligent efforts to improve the employment eligibility verification system.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "A. T. Fragomen, Jr.", written in a cursive style.

Austin T. Fragomen, Jr.
